

# OPINIO JURIS

## in Comparatione

### Studies in Comparative and National Law

Vol. 2, n. 2/2025

#### Section 1 Articles

Cinematic Experience in the Digital Age: addressing regulatory challenge, *Jacopo Fortuna – Nicoletta Patti*

EU data protection liability: the exemption clause ex art. 82 GDPR under the European Court of Justice interpretation and the limits of harmonisation, *Andrea Blatti*

#### Section 2

Special issue on "Towards a multilevel and interdisciplinary assessment for a safer use of digital services and AI-based products", edited by *D. Amram - C. Novara - M. Ratti*

# TABLE OF CONTENTS

## Section 1

- JACOPO FORTUNA and NICOLETTA PATTI, Cinematic Experience >>1  
in the Digital Age: addressing regulatory challenges
- ANDREA BLATTI, EU data protection liability: the exemption clause >>53  
ex art. 82 GDPR under the European Court of Justice interpretation  
and the limits of harmonisation

## Section 2

Special issue on "Towards a multilevel and interdisciplinary assessment for a safer use of digital services and AI-based products", edited by D. Amram - C. Novara - M. Ratti

- DENISE AMRAM, CINZIA NOVARA AND MATILDE RATTI, >>103  
Introduction
- NICOLETTA PATTI, VERONICA PUNZO AND ROBERTA ROMANO, >>107  
Child vulnerabilities in the digital environment: comparative  
insights and operational guidelines
- SARA RIGAZIO, Yes, we can...and we must! changing the narrative >>173  
of children's rights protection in the digital environment through a  
child-centered approach. the lesson from the u.k. children's code
- ALBERTO JACI, Minor's contractual autonomy in the digital >>203  
ecosystem: legal protection and self-determination in private law
- FEDERICA CASAROSA AND LAVINIA VIZZONI, Let's play together: >>217  
fair rules for minor video gamers a research agenda
- SARA TIBIDÒ, NADIA SPATARI, SARA LILLI and MARIA VITTORIA >>237  
ZUCCA, A story of and for children: the lifecycle loop of child  
rights-based AI
- MATILDE RATTI, Il minore nell'era dell'intelligenza artificiale: >>266  
questioni aperte sul metodo di gestione del rischio

"SECTION II"  
SPECIAL ISSUE

*Towards a multilevel and interdisciplinary assessment for a  
safer use of digital services and AI-based products*

**Edited by D. Amram, C. Novara, M. Ratti**

## **INTRODUCTION TO THE SPECIAL ISSUE ON "TOWARDS A MULTILEVEL AND INTERDISCIPLINARY ASSESSMENT FOR A SAFER USE OF DIGITAL SERVICES AND AI-BASED PRODUCTS"**

Denise Amram, Cinzia Novara, Matilde Ratti

### **Abstract**

This is a short introduction to a special issue resulting from research conducted in the last two years, dealing with the development of a multilevel assessment for digital services and AI-based products with the lenses of children's rights.

### **Keywords**

Digital services – AI Systems – Children's Rights.

### **Introduction**

In the last years, the EU Commission approved a series of legislative initiatives aiming to address the fundamental rights and societal values within the new mechanisms imposed by the digitalisation of services and products.

Starting from the approval of the EU Regulation n. 2016/679 on General Data Protection Regulation, pursuing to the EU Regulation n. 2022/2065 on Digital Services Act, and the EU Regulation n. 2024/1689 on AI Act, the so-called risk-based approach has become part of the current compliance procedures both for private organisation and public institutions. This encouraged an interdisciplinary dialogue aiming to translate into organisational and technical measures considering the level of protection and the nature of the activities carried out on a case-by-case basis.

At the same time, users are required to develop tailored technical and soft skills to become everyday more aware and responsible consumers, or data subjects, or users of a given digital service or product.

In this complex context, we decided to investigate the urgency to take in due consideration the vulnerabilities that especially younger users may face every day, while dealing with new technologies and / or within the digital environment.

The initial legal challenge immediately required to be completed by an interdisciplinary approach, opening to the psycho-educational and relational dynamics in order to better address the stratification of possible scenarios and the corresponding implications both in terms of risks and opportunities and policy-making contribution. Users, in fact, may play a proactive role, or being just a passive character, depending on the nature of the given service or product, on the age, grade of autonomy, personal skills and competence, and also on the relational and educational frame they are living in.

Our research dealt with the analysis of the regulatory framework to be compared with practical scenarios and empirical data generated through tailored participatory activities. From the multilevel assessment, interpretative gaps and enablers allowed to draft and validate policy and recommendations for a safer use of digital services and products applied to different stakeholders - including policy-makers, professionals, economic operators, families, and the target group (*i.e.* children) - considering the ethical-legal-technical frameworks, as well as the needs emerging from the psycho-educational domain.

The first paper of this special issue illustrates and comments the developed policies and recommendations under a comparative law perspective (N. Patti, V. Punzo, R. Romano "*Child Vulnerability in the Digital Environment: Comparative Insights and Operational Guidelines*"). In addition, in order to extend the open discussion on the project outcomes, we collected a series of articles selected through a call for papers launched within the project life-cycle among the relevant scientific communities.

We selected proposals concerning possible comparative and private law perspectives addressed both to the economic stakeholders (services providers, digital platforms, AI-based systems developers and deployers), and to the target group (children) and their families, dealing with the empowerment of children's fundamental rights (S.

Rigazio “*Yes, We Can.. and We Must! Changing the Narrative of Children’s rights Protection in the Digital Environment through a Child-Centred Approach. The lesson From the UK Children’s Code*”), looking also at the contractual dimension of private law relationships (A. Jaci “*Minors’ Contractual Autonomy in the Digital Ecosystem: Legal Protection and Self-Determination in Private Law*”), and the playful one (F. Casarosa – L. Vizzoni “*Let’s play together: fair rules for minor video gamers*”). Finally, the fourth paper deals with the life-cycle design of an AI-based product, providing insights from an ethical-legal and technical perspective (S. Tibidò, N. Spatari, S. Lilli, and M.V. Zucca “*A Story of and for Children: The Lifecycle Loop of Child Rights-Based AI*”).

The special issue is completed with a systematic reconstruction of the challenges faced and the methodologies developed in the project, oriented to properly review the legal measures adopted at international, European, and national levels for children’s protection in the digital environment, with specific regard to the use of AI (M. Ratti “*Il minore nell’era dell’intelligenza artificiale: questioni aperte sul metodo di gestione del rischio*”).

We are grateful to all the contributors as they raised original analysis to propose interpretations for a safer digital environment and a more responsible use of new technologies, by encouraging actions aiming to promote and enhance children’s rights.

### **Acknowledgements**

This special issue has been developed in the context of the project titled *Children as vulnerable users of IoT and ai-based technologies: a multi-level interdisciplinary assessment* (CURA), funded by the Italian Ministry of University and Research under the PRIN 2022 programme – Next Generation EU; CUP: J53D23005540006.



## CHILD VULNERABILITIES IN THE DIGITAL ENVIRONMENT: COMPARATIVE INSIGHTS AND OPERATIONAL GUIDELINES

Nicoletta Patti, Veronica Punzo, Roberta Romano\*

### Abstract

The article investigates the condition of child vulnerability in the digital environment through a legal and comparative lens, aiming to reconcile protection with the recognition of children's evolving capacities. Embracing the concept of vulnerability as a dynamic and multilayered notion, it analyses how European regulatory instruments such as the GDPR, the Digital Services Act and the Artificial Intelligence Act address children's rights within a risk-based governance framework.

The discussion is enriched by a comparative analysis of the United Kingdom and France, whose regulatory models offer advanced examples of child-centred and participatory digital regulation. Particular attention is devoted to the online search for origins by adopted minors, a paradigmatic case where digital exposure intersects with identity-related and emotional vulnerability.

Building on these insights, the paper formulates operational guidelines and policy recommendations directed at legislators, institutions, professionals, and industry actors. Ultimately, it argues that digital literacy and education constitute the cornerstone of a rights-based approach capable of transforming child vulnerability into agency and fostering a genuinely inclusive digital citizenship.

---

\* This paper is the result of a common research and reflection of the authors. However, within the scope of research evaluations, Nicoletta Patti drafted Sections 1, 2, 3, 4; Roberta Romano drafted Sections 5, 5.1, 6 and Veronica Punzo, Sections 7, 8, 9. The conclusions were co-authored.

This contribution has been developed within the framework of the PRIN 2022 project – *Children as Vulnerable Users of IoT and AI-based Technologies: A Multi-level Interdisciplinary Assessment* – CURA, PRIN 2022–2022KAEWYF, – Next Generation EU; CUP: J53D23005540006 Double blind peer reviewed contribution.

## Table of Contents

CHILD VULNERABILITIES IN THE DIGITAL ENVIRONMENT: COMPARATIVE INSIGHTS AND OPERATIONAL GUIDELINES .....	107
Abstract.....	107
Keywords.....	108
1. The Vulnerabilities of Minors in the Digital Environment.....	109
2. The European Regulatory Framework.....	113
3. Comparative Insights from the United Kingdom and France.....	118
4. Principles in Action: Building a Digital Environment <i>for</i> and <i>with</i> Children... ..	124
5. The complex balance between privacy preserving and search for origins .....	131
5.1 Towards a responsible approach: lessons learnt from the French and UK systems .....	137
6. Search for origin on digital environment: take away recommendations.....	141
7. Digital Education as a Response to (not only digital) Vulnerability: educational practices and regulatory frameworks .....	151
8. The role of educational institutions and educational alliances: a comparison between Italy, United Kingdom, and France.....	158
9. Bridging the digital divide: empowering online safety through digital education .....	167
10. Conclusions.....	169

## Keywords

Child Vulnerabilities – Digital Environment – Education – Adoption – Comparative Law

## 1. The Vulnerabilities of Minors in the Digital Environment

In the contemporary digital context, technological development has opened unprecedented avenues for expression, learning and participation. At the same time, however, it has intensified forms of exposure to risk, relational dependency and informational asymmetry, particularly affecting those in structurally fragile conditions. In this regard, the condition of minors is emblematic: as individuals in the process of development, they embody an ontological vulnerability that, in legal terms, translates into a complete incapacity<sup>1</sup>. This legal status has traditionally been associated with a protective approach, which aims to shield children from harm through the limitation of their decision-making power.

Alongside this protective perspective – which, though grounded in legitimate concerns, risks producing exclusionary effects – a complementary perspective has gained increasing prominence. This approach recognizes and values children's evolving capacities, affirming their right to active participation and progressive autonomy, especially within digital environments.

Building on this conceptual shift, two interrelated questions have persistently guided our research and defined its normative horizon: how can children's rights be not only formally acknowledged but also effectively guaranteed within digital environments? And how can the imperative of protection be reconciled with the recognition of children's evolving capacities, thus enabling meaningful forms of autonomy and agency in their online interactions?

These foundational questions compel a preliminary conceptual clarification of the notion of vulnerability. Now central to contemporary legal and political discourse, vulnerability constitutes a crucial interpretive lens through which to examine the tension between protection and autonomy that defines the digital condition of childhood and adolescence. As early as 1989, Robert Chambers noted the pervasive yet often imprecise use of the term in development studies, highlighting its conceptual elasticity<sup>2</sup>. Vulnerability should not be understood as a monolithic or merely descriptive category; rather, it denotes a condition of heightened exposure to harm,

---

<sup>1</sup> For a general overview, D. Amram, *Children (in the digital environment)*, in *Elgar Encyclopaedia of Law and Data Science*, G. Comandé (dir.), Elgar, 2022, pp. 155 ff.

<sup>2</sup> R. Chambers, *Editorial Introduction: Vulnerability, Coping and Policy*, in *IDS Bulletin*, vol. 20, 1989, pp. 1 ff.

dependency, or suffering, one that can assume diverse forms and operate across multiple, intersecting dimensions.

Recent legal and ethical scholarship has underscored the need to disaggregate the concept, distinguishing between layered and overlapping vulnerabilities that produce complex scenarios requiring differentiated responses<sup>3</sup>. Among the most influential contributions in this regard is the framework elaborated by Florencia Luna, who introduced the concept of “layers of vulnerability” capturing vulnerability as a dynamic, stratified and context-specific phenomenon<sup>4</sup>.

Particularly relevant is the conceptual distinction between inherent and situational vulnerability. The former is embedded in the human condition itself, encompassing universal dimensions such as corporeality, relationality and constitutive dependency. The latter, by contrast, arises from contextual factors (economic, social, cultural, technological) or from personal histories and characteristics that heighten exposure to risk. These layers often intersect, producing complex constellations of vulnerability that require equally nuanced normative and policy responses.

In the context under consideration, developmental age represents a paradigmatic form of intrinsic vulnerability. However, digital environments can amplify situational vulnerabilities linked to limited digital literacy, manipulative design architectures, exposure to inappropriate or distressing content, the absence of adequate familial or educational scaffolding and the lack of effective legal and technical safeguards. In certain cases, dispositional vulnerabilities may also come into play, stemming from personal traits or life experiences that render some children more susceptible to harm. This is particularly true for adopted minors, whose condition frequently involves

---

<sup>3</sup> W. Rogers, C. Mackenzie, S. Dodds, *Why Bioethics Needs a Concept of Vulnerability?*, in *International Journal of Feminist Approaches to Bioethics*, vol. 5, n. 2, 2012, pp. 11-38. For a conceptual application of the multidimensional (or stratified) taxonomy of vulnerability in the specific context of the interaction between minors and AI-powered toys, see: A. Pera, S. Rigazio, *Let the Children Play. Smart Toys and Child Vulnerability*, in C. Crea, A. De Franceschi (a cura di), *The New Shapes of Digital Vulnerability in European Private Law*, Elgar, 2024, pp. 413-437.

<sup>4</sup> Although originally developed in the context of bioethical debates, Luna’s theory of layered vulnerability offers a conceptual framework that proves equally valuable when applied to the digital environment and the specific challenges it poses to children’s rights and protection. F. Luna, *Elucidating the Concept of Vulnerability: Layers Not Labels*, in *International Journal of Feminist Approaches to Bioethics*, vol. 2, n. 1, 2009, pp. 121-139, <http://www.jstor.org/stable/40339200>.

identity-related, emotional and relational fragilities that may be intensified, or instrumentalized, within digital contexts<sup>5</sup>.

It thus becomes evident that among vulnerable individuals, some may be more vulnerable than others<sup>6</sup>. Recognizing the factors that shape individual fragility is essential for devising effective protective and empowering measures. The objective is not to crystallize categories, but rather to identify with precision those conditions that render an individual, particularly a child, more or less exposed to harm, in order to formulate tailored and proportionate responses. In this perspective, vulnerability should not serve as a justification for paternalistic or exclusionary interventions based solely on prohibition. Instead, it should function as an interpretive lens for building relational contexts that reinforce individual capabilities, foster autonomy and enable informed, meaningful participation.

A multidimensional understanding of vulnerability therefore calls for a departure from fragmented or siloed approaches and for the development of integrated normative frameworks that recognise children not as passive recipients of protection, but as rights-holders entitled to the effective enjoyment of interconnected rights, such as privacy, identity and participation, particularly in digital settings. From this vantage point, vulnerability does not signify incapacity; rather, it demands a collective and institutional responsibility to construct inclusive environments where protection and empowerment are not oppositional but mutually reinforcing.

This framework is firmly grounded in the Convention on the Rights of the Child<sup>7</sup>, which inaugurated a paradigmatic shift in the legal understanding of childhood. No longer construed merely as subjects in need of protection, children are now recognised as autonomous rights-holders, endowed with intrinsic dignity and agency. Article 12 of the Convention is particularly emblematic in this regard: it enshrines the

---

<sup>5</sup> Cf. Sections 5-7 of this contribution.

<sup>6</sup> F. Luna, *Identifying and evaluating layers of vulnerability – a way forward*, in *Developing World Bioethics*, vol. 19, n. 2, 2019, p. 87. This conception of vulnerability as a dynamic and context-dependent condition can also be found in several policy documents issued by the European Commission in the field of consumer protection. Notably, the Commission acknowledges that “*consumer vulnerability is situational, meaning that a consumer can be vulnerable in one situation but not in others, and that some consumers may be more vulnerable than others*”, European Commission, *Understanding consumer vulnerability in the EU’s key markets*, Factsheet, Brussels, 2016, Available at: [https://commission.europa.eu/system/files/2018-04/consumer-vulnerability-factsheet\\_en.pdf](https://commission.europa.eu/system/files/2018-04/consumer-vulnerability-factsheet_en.pdf).

<sup>7</sup> Convention on the Rights of the Child, New York, 1989.

right of every child capable of forming their own views to express those views freely in all matters affecting them and requires that due weight be given to such views in accordance with the child's age and maturity. This provision not only reinforces the overarching principle of the best interests of the child but also lays the foundation for their meaningful participation in social, legal and institutional decision-making processes.

The United Nations Committee on the Rights of the Child, with its General Comment No. 25 (2021)<sup>8</sup>, has further elaborated on the application of these principles within digital environments. It calls for an approach that respects children's evolving capacities, ensures age-appropriate protective measures, promotes digital literacy among caregivers and imposes robust obligations on digital service providers to uphold high standards of transparency, privacy and safety. In doing so, the Committee emphasises that digital engagement must be guided not only by the imperative to protect, but also by the commitment to empower children as active participants in the shaping of their digital experiences.

The approach adopted in the following pages builds on this foundation. The analysis begins with a review of the EU regulatory framework and the most advanced national strategies – notably those of the United Kingdom and France – to examine how they address the vulnerabilities of minors in digital environments, highlighting critical issues, good practices and areas for improvement<sup>9</sup>.

The overarching aim is to promote a genuinely child-centred approach, one that transcends the abstract articulation of principles and translates them into concrete, actionable and widely shared practices. This requires establishing an operational horizon grounded in effective, multi-level co-responsibility among all stakeholders – children, families, institutions, practitioners, and industry actors – called upon to

---

<sup>8</sup> General comment n. 25 (2021) on children's rights in relation to the digital environment.

<sup>9</sup> A series of *Blueprint Guidelines* have been developed with the contribution of the Authors within the PRIN 2022 Italian MUR Project *Children as Vulnerable Users of IoT and AI-based Technologies: A Multi-level Interdisciplinary Assessment – CURA* (hereinafter also *CURA Blueprint*), n. KAEWYF, V03. These policy proposals are the outcome of an interdisciplinary and inter-institutional consultation involving legal scholars, psychologists, and educators, with the overarching goal of integrating the protection of privacy with minors' rights to participation and their progressive development of autonomy. This paper refers to the aforementioned *Blueprint Guidelines*, which were first drafted as part of Deliverable D6, "First Version of the Blueprint Guidelines", and subsequently refined through the validation process. The final version is available at: [https://www.lider-lab.it/wp-content/uploads/2025/10/PRIN-CURA\\_Blueprint-Policies-and-Guidelines\\_final.pdf](https://www.lider-lab.it/wp-content/uploads/2025/10/PRIN-CURA_Blueprint-Policies-and-Guidelines_final.pdf).

cooperate within their respective roles and competences to ensure and actualize the rights of children in digital environments.

Within this setting, the article delves into the specific condition of adopted children, a context in which vulnerabilities often become more complex and layered. Indeed, this case study exemplifies how intrinsic and situational vulnerabilities can intersect and intensify, leading to heightened exposure to risk and requiring the adoption of targeted protective measures. Consequently, particular attention is devoted to the search for biological origins in the digital environment, considering both the emancipatory potential and the risks associated with such deeply personal and identity-sensitive journeys involving the sharing of data and personal information (see *infra*, sections 5, 5.1 and 6).

Finally, digital literacy and education are examined as strategic levers for the empowerment of minors and for raising awareness within families and society at large. These dimensions cut across all levels of intervention and are essential for equipping all stakeholders with the tools needed to navigate digital environments safely, critically and responsibly (see sections 7, 8 and 9).

## **2. The European Regulatory Framework**

The European legal framework has progressively broadened its focus on protecting minors in the digital environment, outlining a complex, multi-layered regulatory architecture aimed at fostering safe and accessible digital spaces. The overarching goal, in line with the principles enshrined in the UN Convention on the Rights of the Child (hereinafter UNCRC), is to foster an environment in which children can actively and consciously exercise their rights, including the right to protection, participation, and harmonious development.

One of the fundamental pillars of this system is Regulation (EU) 2016/679 (General Data Protection Regulation, hereinafter GDPR)<sup>10</sup>, which, although not specifically addressed to minors, explicitly recognises their vulnerability (Recital 38), requiring

---

<sup>10</sup> Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679>.

enhanced protection of their personal data. The GDPR adopts a risk-based approach aimed at assessing the impact of each element of the processing - means, purposes, nature of the data, technology and actors involved - on the individual. Central to this logic is Article 25, which enshrines the principle of data protection by design and by default, requiring data protection measures to be integrated from the outset of system design, with particular attention to the rights and freedoms of data subjects. With specific regard to children, Article 8 sets the default age of digital consent at 16, while allowing Member States to lower this threshold to 13. Italy has opted for a lower age, setting it at 14<sup>11</sup>. Under the GDPR, data controllers are required to make reasonable efforts to verify that consent has been validly given by the holder of parental responsibility<sup>12</sup>. The Regulation also imposes strict obligations concerning transparency, accessibility, and age-appropriate language (Articles 12 and 13), placing particular emphasis on the comprehensibility of the information provided and on the child's awareness of their own rights<sup>13</sup>. However, the framework outlined by the GDPR does not take into account the child's evolving capacity for discernment, thereby neglecting the differences among the various stages of child and adolescent development and flattening the assessment of individual maturity to the mere formal criterion of age.

While the GDPR focuses primarily on the protection of personal data, the European Union has broadened its regulatory efforts to address the systemic risks of the digital ecosystem. In 2022, it adopted Regulation (EU) 2022/2065, known as the Digital

---

<sup>11</sup> See Article 2-quinquies of the Italian Data Protection Code (Legislative Decree n. 196/2003, as amended by Legislative Decree No. 101/2018), available at: <https://www.gazzettaufficiale.it/eli/id/2018/09/04/18G00129/sg>.

<sup>12</sup> In this vein, the European Data Protection Board (EDPB) issued Declaration 1/2025 on Age Verification, adopted on 11 February 2025. The declaration offers detailed guidance on designing age verification systems that are compliant with the GDPR. Among the recommended practices are tokenized verification through trusted third parties, age band verification mechanisms capable of tailoring protective measures to the child's developmental stage, and multifactorial models (e.g., biometric estimation combined with parental consent), which seek to balance effectiveness, accuracy, and privacy protection. The declaration thus aligns with broader child-centred European strategies, reaffirming the commitment to harmonize the protection of minors with a regulatory framework grounded in constitutional and supranational principles on fundamental rights. Available at: [https://www.edpb.europa.eu/system/files/2025-04/edpb\\_statement\\_20250211ageassurance\\_v1-2\\_en.pdf](https://www.edpb.europa.eu/system/files/2025-04/edpb_statement_20250211ageassurance_v1-2_en.pdf).

<sup>13</sup> See D. Amram, *Children (in the digital environment)*, cit., pp. 64 ff.

Services Act (DSA)<sup>14</sup>, marking a crucial step towards a more accountable governance of online intermediaries. The DSA, once again, is not specifically dedicated to children, yet it acknowledges their vulnerability in multiple provisions and imposes enhanced obligations on service providers – particularly very large online platforms (VLOPs), which are frequently used by children and adolescents (such as TikTok, Instagram and Snapchat) – with regard to algorithmic transparency, fundamental rights impact assessments and the prohibition of targeted advertising to minors. As in the GDPR, the concept of risk functions as a core regulatory principle within the DSA, shaping the structure of obligations and safeguards across the text. Articles 34 and 35 require very large online platforms to conduct both *ex ante* and continuously updated risk assessments, especially regarding systemic risks to fundamental rights. Article 28 mandates the adoption of adequate and proportionate measures to safeguard minors, particularly in terms of privacy and safety, including a ban on advertising interfaces based on profiling. Articles 12 and 44 reinforce the obligation to ensure clear, accessible communication and targeted protection for children and adolescents as especially vulnerable users. Article 45 also envisages the development of a Code of Conduct. The DSA’s regulatory architecture is therefore centred on safeguarding individuals as users and consumers of digital services and operates in a complementary fashion to the broader privacy protection framework established by the GDPR.<sup>15</sup>

The reference to minors has been further consolidated in Regulation (EU) 2024/1689 on Artificial Intelligence<sup>16</sup> (commonly known as the AI Act), which introduces, for the first time in a binding legal text, a systematic use of the concept of “vulnerability” (appearing 19 times, including 7 within the operative provisions)<sup>17</sup>. In particular,

---

<sup>14</sup> Regulation (EU) 2022/2065 on a single market for digital services and amending Directive 2000/31/EC (Digital Services Act), available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=LEGISSUM:4625430>.

<sup>15</sup> D. Amram, *Children (in the digital environment)*, cit., pp. 64 ff.

<sup>16</sup> Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) n.300/2008, (EU) n. 167/2013, (EU) n. 168/2013, (EU) n. 2018/858, (EU) n. 2018/1139 and (EU) n. 2019/2144 and Directives n. 2014/90/EU, (EU) n. 2016/797 and (EU) n. 2020/1828 (Artificial Intelligence Act). Available at: [https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L\\_202401689](https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401689).

<sup>17</sup> For a detailed discussion of how the concept of vulnerability is addressed in the AI Act, see: M.L. Rebream, G. Malgieri, *Vulnerability in the EU AI Act: building an interpretation*, in *FAaT '25: Proceedings of the 2025 ACM Conference on Fairness, Accountability, and Transparency*, November 28, 2024, pp. 1985-1997, available at

among others, recital 28 acknowledges children as vulnerable subjects deserving enhanced protection, while Article 5(1)(b) explicitly prohibits the use of AI systems designed to exploit their cognitive vulnerabilities, such as manipulative interactive toys or persuasive interfaces. AI systems used in educational settings are classified as high-risk and are therefore subject to stringent governance and oversight requirements (Annex III, Article 6). Additional key provisions (Articles 7(h), 27, 29(2), and 60(4)(g)) address safeguards in regulatory sandboxes and establish specific guarantees where AI systems may affect vulnerable individuals, including minors, thus reinforcing the internal coherence of the regulatory framework with the risk-based approach. In this sense, the principle of risk management, already central to both the GDPR and the DSA, thus resurfaces prominently in the AI Act, evidencing the transversal consistency of European digital regulatory strategies.

It should be noted, however, that although the AI Act marks a significant step forward by introducing the notion of vulnerability into binding legislation and including children within certain key provisions (e.g., Article 5(1)(b)), the overall protection of minors remains fragmented: direct references to children's rights are largely confined to the recitals and the normative provisions do not consistently reflect a child-centred approach, leaving their effective protection uncertain and reliant on broad interpretations<sup>18</sup>.

This uneven recognition of children's needs within the AI Act must be situated within a broader normative and policy trajectory. In particular, the regulatory framework draws upon the strategic vision already articulated in the European Commission's Communication of 11 May 2022, "*A Digital Decade for Children and Youth: the new European strategy for a Better Internet for Kids (BIK+)*"<sup>19</sup>, which provides a more holistic

---

SSRN: <https://ssrn.com/abstract=5058591>; F. Galli, C. Novelli, *The Many Meanings of Vulnerability in the AI Act and the One Missing*, in *BioLaw*, vol. 1, 2024, pp. 53 – 72, available at <https://doi.org/10.15168/2284-4503-3302>; G. Malgieri, *Human vulnerability in the EU Artificial Intelligence Act*, in Oxford University Press blog.

<sup>18</sup> For a comment see: S. Lindroos-Hovinheimo, *Children and the Artificial Intelligence Act: Is the EU Legislator Doing Enough?*, in *European Law Blog*, 2024. See also: 5rightsfoundation, [EU adopts AI Act with potential to be transformational for children's online experience](#).

<sup>19</sup> Available at: <https://digital-strategy.ec.europa.eu/it/policies/strategy-better-internet-kids#:~:text=La%20nuova%20strategia%20per%20un,di%20bambino%20della%20strategia%20BIK%2B>.

It should be noted that as early as 2012 the European Commission launched the first *Better Internet for Kids (BIK)* strategy, structured around four main pillars: the promotion of high-quality online content for children, the empowerment and awareness-raising of minors, the creation of a safer digital environment, and the fight against online child sexual abuse and the dissemination of child sexual abuse material (available at: <https://eur-lex.europa.eu/eli/legislation/2012/339/it>).

and programmatic foundation for child protection in digital environments. The strategy – structured around three core pillars: a safe digital environment, digital empowerment and active participation - calls on platforms to adopt accessible and transparent design practices, conduct systemic risk assessments and implement safeguards against content potentially harmful to the mental, physical, or moral well-being of minors. A key initiative under the BIK+ strategy is the forthcoming EU Code of Conduct on Age-Appropriate Design (the 'BIK+ Code'), which seeks to operationalise art. 45 of the DSA. The Code will also be aligned with the broader EU legal framework and will aim to strengthen industry's responsibility in safeguarding children's privacy, safety and well-being online.

The drafting process has been entrusted to a special ad hoc group composed of representatives from industry, academia and civil society<sup>20</sup>. In line with the participatory aims of the BIK+ strategy, children and young people are also expected to be involved in the working group, ensuring that their perspectives contribute to shaping a regulatory instrument genuinely responsive to their needs and rights<sup>21</sup>.

Overall, the European framework demonstrates an increasing awareness of the condition of minors in the digital environment. However, a degree of fragmentation persists among binding legal instruments (such as the GDPR, the DSA and the AI Act), soft law tools and sectoral strategies. While the explicit recognition of children's vulnerability is undoubtedly significant, it risks remaining confined to a precautionary logic unless accompanied by genuine normative integration and coherent, inclusive and enabling political action.

In this perspective, a qualitative leap appears essential – towards a model of shared responsibility involving public institutions, private actors and civil society – to foster a digital environment that truly respects the rights of the child.

---

[lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52012DC0196](https://lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52012DC0196)). The 2022 version, BIK+, represents a comprehensive update of that strategy, in line with the evolving challenges of the digital environment and the goals of the European Digital Strategy and the EU Strategy on the Rights of the Child.

<sup>20</sup> The list of members is publicly accessible on the European Commission's website: <https://digital-strategy.ec.europa.eu/en/news/members-special-group-eu-code-conduct-age-appropriate-design>. The first meeting of the dedicated expert group for the development of the EU Code of Conduct on age-appropriate design took place on 13 July 2023. See: <https://digital-strategy.ec.europa.eu/en/library/meetings-special-group-eu-code-conduct-age-appropriate-design>.

<sup>21</sup> See: <https://digital-strategy.ec.europa.eu/en/policies/group-age-appropriate-design>.

Against this backdrop, engaging with the regulatory experiences of other European countries, particularly the United Kingdom and France, offers valuable insights into innovative solutions and complementary approaches that may enrich the ongoing debate on the future of child protection in the digital age.

### **3. Comparative Insights from the United Kingdom and France**

Among the countries that have most decisively embraced a child-centred and design-based approach to digital regulation, the United Kingdom stands out as a pioneering example. The adoption of the Age-Appropriate Design Code<sup>22</sup> (commonly known as the Children's Code), which came into force in 2020, marked a paradigmatic shift in embedding children's rights within the design of digital services<sup>23</sup>. Issued by the Information Commissioner's Office (ICO)<sup>24</sup>, the Code sets out 15 design standards addressed to providers of online services "likely to be accessed by children" (consider, for instance, video games, social networks...). The Code aspires to embed safeguards that protect children within the digital environment, rather than seeking to restrict or prevent their access to it.<sup>25</sup>

The Code explicitly incorporates the principle of the best interests of the child (Standard 1), mandating that organisations prioritise children's rights over commercial considerations. It also gives concrete effect to the principle of evolving capacities (Standard 3), requiring service design to be tailored to different age groups and functionalities that support children's understanding and progressive self-determination. Among the most significant standards are the requirement to keep

---

<sup>22</sup> See: <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/age-appropriate-design-a-code-of-practice-for-online-services/>.

<sup>23</sup> The Code has been developed pursuant to Section 123 of the Data Protection Act 2018, which mandates the Information Commissioner to issue a code of practice providing guidance on the standards of age-appropriate design for information society services that are likely to be accessed by children. The provision entrusts the Commissioner with defining the criteria deemed most suitable to ensure that digital services align with the specific needs and vulnerabilities of underage users.

<sup>24</sup> The ICO is the UK's independent authority responsible for data protection. See: <https://ico.org.uk>.

<sup>25</sup> For an in-depth and comparative analysis of the UK Age-Appropriate Design Code and its potential as a regulatory model beyond the British context, see: S. Rigazio, *L'Empowerment del minore nella dimensione digitale*, Modena, 2024, available in open access at: <https://mucchieditore.it/wp-content/uploads/Open-Access/Rigazio-Prospettive-8-DEF-OA.pdf>.

geolocation services turned off by default (Standard 10), the automatic activation of the highest privacy settings for child users (Standard 7) and the prohibition of manipulative or persuasive techniques, such as dark patterns, that encourage excessive data sharing (Standard 12). Other key principles include transparency (Standard 4), data minimisation (Standard 8), limits on profiling (Standard 11) and the provision of simple and effective tools for children to exercise their digital rights (Standard 15). The Code also mandates the conduct of a data protection impact assessment (Standard 2) and expressly prohibits any data processing likely to harm the physical, mental, or emotional well-being of the child (Standard 5).

As has been noted, “all the standards are characterised by a dual dimension: they are structured according to a by-design approach and are grounded in the principles underpinning the UNCRC”<sup>26</sup>.

Consistent with the overarching European regulatory philosophy, this Code may serve as a paradigmatic reference for the design and implementation of the forthcoming BIK+ Code, which is currently in the drafting phase<sup>27</sup>.

This regulatory landscape is complemented by the more recent *Online Safety Act*, which entered into force in 2023<sup>28</sup>. The Act imposes risk assessment and mitigation duties on digital intermediaries, with a specific focus on content accessibility for children. It designates Ofcom<sup>29</sup> as the regulatory authority, granting it broad oversight and enforcement powers and establishes stringent obligations for digital platforms concerning the prevention, identification and mitigation of online risks to child safety.

Among the Act’s most salient provisions is the mandatory preparation of Children’s Risk Assessments (Section 11), requiring providers to evaluate the risks associated

---

<sup>26</sup> S. Rigazio, *L’Empowerment del minore nella dimensione digitale*, *cit.*, p. 21; translation by the author. For an in-depth analysis of the by-design approach adopted by the Code and its alignment with the principles of the UN Convention on the Rights of the Child see *Id.*, pp. 21–34.

<sup>27</sup> Notably, the Code has already inspired processes of legal circulation and imitation, as demonstrated by the adoption of the California Age-Appropriate Design Code. For a comparative analysis, see: M. Comite, *Prevent Phishy Business: Comparing California’s and the United Kingdom’s Age-Appropriate Design Code to Protect Youth from Cybersecurity Threats*, in *University of Miami International & Comparative Law Review*, vol. 31, 2023, pp. 175–200; E. Lampmann-Shaver, *Privacy’s Next Act*, in *Washington Journal of Law, in Technology & Arts*, vol. 19, n. 1, 2024, pp. 97–129.

<sup>28</sup> UK Parliament, *Online Safety Act*, 2023. <https://www.legislation.gov.uk/ukpga/2023/50>.

<sup>29</sup> See Ofcom’s role under the *Online Safety Act*: <https://www.ofcom.org.uk/online-safety>.

with content, functionalities and digital interactions likely to affect minors. These assessments must be accompanied by proportionate safety measures (Section 12), including the design of algorithms and user interfaces aimed at minimising potential harm. Furthermore, the legislation requires the implementation of reliable age verification or estimation systems (Sections 12.4–6), designed to prevent children from accessing harmful content.

In this regard, the Act offers a precise definition of “primary priority content” (e.g. material promoting self-harm or suicide) and introduces strict requirements relating to transparency (Section 22) and platform accountability. The regulatory framework as a whole seeks to strike a careful balance between child protection, freedom of expression and the right to privacy, while consistently grounding the imposed measures in the principles of proportionality and necessity.

The UK model stands out as one of the most comprehensive and coherent approaches at the European level, successfully combining *by design* principles, data protection and content regulation within a distinctly child-centred perspective. It is further distinguished by the cultural ambition underpinning it. Through the work of the ICO and other institutional actors, the United Kingdom has promoted a transversal strategy of digital literacy aimed not only at children but, crucially, also at adults: parents, educators, social workers, volunteers, local administrators and public officials. In this way, the protection of minors in the digital environment is framed as a collective responsibility, grounded in the cultivation of a widespread, informed and child-respectful digital culture.

Equally significant is the commitment to directly involve children in decision-making processes. Their views are gathered through public consultations and advisory groups, meaningfully contributing to policy design and platform development. This represents a fundamental shift from a paternalistic regulatory logic to a genuinely participatory perspective, rooted in co-creation *with* children rather than mere protection *for* children<sup>30</sup>.

Within this framework, the British model offers an advanced example of child-centred regulation, one that integrates legal safeguards, digital empowerment and

---

<sup>30</sup> ICO, Guidelines on Data Sharing, in <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-sharing/a-10-step-guide-to-sharing-information-to-safeguard-children/>.

social inclusion, thereby providing a valuable benchmark for comparative legal and policy analysis.

In recent years, France has also intensified its institutional and regulatory focus on the condition of minors in the digital environment, with particular attention to the issue of early and prolonged exposure to screens. In January 2024, a national commission was established with the mandate to analyse the impact of digital technologies on the physical and mental health of children, assess the effectiveness of existing measures and formulate concrete policy proposals. The findings of this work were consolidated in the report *Enfants et Écrans – À la Recherche du Temps Perdu*<sup>31</sup>, published in April 2024, which currently stands as the most comprehensive document produced in France on this topic.

The report offers a clear-sighted and nuanced analysis of the ambivalence inherent in minors' digital experiences. On the one hand, it acknowledges the educational and participatory potential of technology; on the other, it highlights the increasingly well-documented risks to physical health (including sleep disorders, obesity and visual impairment), mental well-being (such as anxiety, depression and social withdrawal), and identity formation within highly stereotyped and commercialized environments. In response, the report proposes a comprehensive strategy structured around six key areas of intervention: (1) combating manipulative design practices; (2) ensuring protection rather than mere control of minors; (3) enabling gradual and age-appropriate access to digital tools and platforms; (4) fostering digital autonomy through targeted education; (5) equipping responsible adults with adequate training; and (6) establishing a robust public governance framework.

Building on these six pillars, the Commission outlines twenty-nine operational proposals that collectively define a broad-spectrum public policy agenda. Particularly innovative are the measures aimed at regulating platform design. Among these, the Commission recommends shifting the burden of proof onto digital service providers regarding the impact of their algorithms, prohibiting harmful design practices, and codifying a new "right to configuration," which would grant users, especially minors, the ability to consciously modify default settings that affect them. The report also calls

---

<sup>31</sup> Commission nationale sur l'exposition des enfants aux écrans, *Enfants et Écrans – À la Recherche du Temps Perdu*, April 2024, available at: <https://www.elysee.fr/admin/upload/default/0001/16/fbec6abe9d9cc1bff3043d87b9f7951e62779b09.pdf>.

for the introduction of effective age verification mechanisms and increased investment in educational content.

Of significant note is the proposal to prohibit screen exposure for children under the age of six within educational settings, to delay access to social media until the age of fifteen, and to adopt a phased approach to the introduction of mobile phones and personal digital devices. This graduated policy suggests: no phones before age 11; basic phones without internet connectivity from age 11; internet-enabled phones from age 13, but with restrictions on social media and illegal content; and from age 15, expanded access to vetted social media platforms. These measures are accompanied by structural interventions within the school environment, aimed at equipping students, educators and families with the critical and pedagogical tools necessary for informed digital citizenship. Digital education is conceived as a cross-cutting dimension to be integrated into pedagogical competencies, mental health curricula, interpersonal relations, emotional regulation and digital risk awareness.

The French legislator had already intervened through a series of fragmented measures. As early as 2010, the legislation on online gambling established a prohibition on access for minors<sup>32</sup>. However, a more substantial regulatory consolidation has been observed since 2022. The so-called *Loi Studer* (2022)<sup>33</sup> introduced a requirement for digital device manufacturers to pre-install free parental control tools. The 2023 law on influencers regulated advertising practices targeting minors, introducing specific

---

<sup>32</sup> Law n. 476/2018, 12 May 2010, relating to the opening up to competition and the regulation of the online gambling and games of chance sector (Loi n. 2010-476 du 12 mai 2010 relative à l'ouverture à la concurrence et à la régulation du secteur des jeux d'argent et de hasard en ligne), available at : <https://www.legifrance.gouv.fr/loda/id/JORFTEXT000022204510>.

<sup>33</sup> Law n. 330/2022, 2 March 2022, aimed at strengthening parental control over means of accessing the Internet (Loi n. 2022-300 du 2 mars 2022 visant à renforcer le contrôle parental sur les moyens d'accès à internet), <https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000045287677>. For a critical reflection on the challenges faced by parents in managing children's digital exposure, see M. Haza-Pery, T. Rohmer, *Enfants connectés, parents déboussolés*, Brussels, 2023.

safeguards for children engaged in “baby influencer” activities<sup>34</sup>. The *Loi Marcangeli*<sup>35</sup> on online hate speech established a so-called “digital age of majority” at fifteen years for access to social media platforms - though this provision has raised concerns regarding its compatibility with European Union law. In 2024, a dedicated law on privacy and image rights of minors was enacted<sup>36</sup>, imposing on parents a legal duty to respect their children's privacy and establishing judicial mechanisms aimed at safeguarding the child's digital identity.

The *Enfants et Écrans* report thus positions itself within an already existing normative framework yet seeks to enhance its systemic coherence by offering an integrated, child-centred vision. At the heart of the report lies the active involvement of children and adolescents: 150 minors were consulted during the Commission's work, and their perspectives were explicitly incorporated into the formulation of the final recommendations<sup>37</sup>. Youth participation, combined with a strong reliance on scientific evidence and the precautionary principle, underpins a model of governance that aims to move beyond emergency-driven responses in favour of a long-term regulatory architecture. In this regard, the report calls for the establishment of a new national governance structure for digital literacy, to be financed through the

---

<sup>34</sup> Law n. 451/2023, 9 June 2023, aimed at regulating commercial influence and combating the excesses of influencers on social networks (Loi n. 2023-451 du 9 juin 2023, visant à encadrer l'influence commerciale et à lutter contre les dérives des influenceurs sur les réseaux sociaux), <https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000047663185>. For a comparative analysis with the UK legal framework, particularly on influencers, labour law and social protection, see C. Marzo, *Influencers, Labour Law and Social Protection: A Comparative Analysis between France and the United Kingdom*, in *The Hashtag Hustle*, Taylor Annabell, Christian Fieseler, Catalina Goanta, and Isabelle Wildhaber (eds.), Edward Elgar, 2025, pp. 130–148.

<sup>35</sup> Law n. 566/2023, 7 July 2023, aimed at establishing a digital majority and combating online hate (Loi n. 2023-566 du 7 juillet 2023 visant à instaurer une majorité numérique et à lutter contre la haine en ligne), <https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000047799533>. M. Saulier, *Loi n° 2023-566 du 7 juillet 2023 visant à instaurer une majorité numérique et à lutter contre la haine en ligne*, in *Actualité juridique Famille*, vol. 9, 2023, pp. 420 ff. ([halshs-04206468](#)).

<sup>36</sup> Law n. 120/2024, 19 February 2024, aimed at ensuring respect for children's image rights (Loi n. 2024-120 du février 2024 visant à garantir le respect du droit à l'image des enfants), [https://www.legifrance.gouv.fr/loda/id/JORFTEXT000049163317/2025-04-16/#:~:text=LOI%20n%202024%2D120,des%20enfants%20\(1\)%20%2D%20L%C3%A9gifrance](https://www.legifrance.gouv.fr/loda/id/JORFTEXT000049163317/2025-04-16/#:~:text=LOI%20n%202024%2D120,des%20enfants%20(1)%20%2D%20L%C3%A9gifrance). For a comment on the effectiveness of France's new rules on children's image rights, see M. Saulier, *Garantir le respect du droit à l'image des enfants: un objectif ambitieux, une efficacité douteuse?*, in *Actualité juridique Famille*, n. 3, 2024, pp. 116 ff. ([halshs-04500845](#)).

<sup>37</sup> Commission nationale sur l'exposition des enfants aux écrans, *Enfants et Écrans – À la Recherche du Temps Perdu*, April 2024, p. 14.

application of the “polluter pays” principle and sustained support for responsible actors, research institutions and widespread educational campaigns.

The French response thus stands out for the breadth and depth of its vision, marked by a strong emphasis on ethical design, child agency and the educational role of civil society. It constitutes an ambitious model that opens up promising avenues for digital child protection across Europe, although its effective implementation and stable coordination with European Union law remain, at least for now, partially pending.

The comparative analysis of legal and regulatory frameworks in the United Kingdom and France has proved especially valuable in identifying alternative or complementary models for safeguarding children in the digital environment. While grounded in distinct legal and institutional traditions, the solutions adopted in these jurisdictions offer meaningful contributions in terms of regulatory strategies, operational mechanisms and the role of independent oversight bodies. Building on these reflections, a set of blueprint policies has been developed, drawing on EU-level principles and integrating national best practices, with the aim of formulating concrete recommendations to enhance the protection of children’s rights in today’s digital landscape.

#### **4. Principles in Action: Building a Digital Environment *for and with* Children**

Adopting a child-centred perspective and drawing on an intrinsic and situational understanding of vulnerability means translating theoretical principles concerning children’s rights, previously analysed, into concrete operational actions capable of guiding educational practices, regulatory frameworks and digital design<sup>38</sup>. Anchoring themselves in the principle of the best interests of the child (Article 3 UNCRC) and in key EU instruments such as the GDPR, the DSA and the AI Act, this framework aims to reconcile privacy protection with the promotion of participation and evolving capacities.

The theoretical architecture underpinning concrete actions is grounded in a non-reductionist conception of vulnerability, understood not as a permanent or

---

<sup>38</sup> The reference is to the *CUR4 Blueprint Guidelines*, cited in note 9, to which the reader is referred for further details.

pathological condition, but rather as a dynamic, context-dependent expression of the interaction between individual and environment, shaped by personal, social and technological factors. Accordingly, responses to vulnerability cannot be confined to paternalistic or purely protective logics; instead, they must pursue a calibrated balance between safeguarding, progressive responsibility and the enhancement of evolving capacities. A dynamic understanding of children's evolving capacities calls for privacy-by-design measures tailored to developmental stages and for the active involvement of minors in shaping their digital environments. In this perspective, protection and empowerment are not opposing aims, but complementary dimensions of the same child-centred framework.

Although this perspective may initially appear more sociological based than legal, regulatory frameworks such as than the UK *Age-Appropriate Design Code* and the French clearly demonstrate that multi-stakeholder cooperation is not merely desirable, but legally indispensable. The UK experience is emblematic: the sanctioning powers vested in the ICO have already produced tangible effects, with substantial fines imposed on major digital platforms, as in the case of TikTok, thereby confirming the normative robustness and the effective enforceability of this model<sup>39</sup>.

The suggested guidelines' evolutionary and plurilateral approach is fully consistent with the legal framework established by the UNCRC, which places the principle of evolving capacities at its core, and with recent case law that increasingly recognises the child's progressive autonomy in exercising rights and in shaping the scope of protective obligations<sup>40</sup>.

Finally, to reinforce the legitimacy of a participatory and multi-level methodology in public policy-making, reference should be made to the recent Colorado AI Act White Paper (2024). Drafted precisely in this spirit, and due to enter into force in 2026, it represents a paradigmatic precedent in comparative law. The document explicitly frames governance not as a mere bureaucratic constraint but as a mechanism of *responsible value creation*, calling for cooperation among developers, deployers and

---

<sup>39</sup> In April 2023, for example, the ICO fined TikTok £12.7 million for misusing children's data, including failing to restrict underage users and processing personal data without parental consent. This is an enforcement decision that concretely underscores the legal force behind the regulatory principles. See *ICO fines TikTok £12.7 million for misusing children's data*: <https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2023/04/ico-fines-tiktok-127-million-for-misusing-children-s-data/>.

<sup>40</sup> For an in-depth analysis, see S. Rigazio, *L'Empowerment del minore nella dimensione digitale*, cit. pp. 124 ff.

regulators. In line with this logic, the Act imposes binding obligations on both developers and deployers of high-risk AI systems, requiring transparency, risk assessment, documentation and continuous monitoring, while encouraging compliance to be shaped as a form of “co-governance” rather than unilateral control. This confirms that participatory governance is no longer a merely theoretical aspiration but has now become a consolidated regulatory technique of growing comparative significance<sup>41</sup>.

Based on these premises, the proposed actions are structured along three key dimensions - technological, ethical-legal and educational-psychological - and are addressed to four main stakeholder groups: families, professionals, public and private organisations, and minors themselves. Their design is inspired also by the advanced regulatory experiences previously discussed, such as the UK’s Age-Appropriate Design Code and recent French strategies, which promote a multi-level approach based on protection by design, shared responsibility and participatory co-creation.

Families are identified as pivotal actors in creating safe and enabling digital environments. Strengthening parents’ digital literacy and awareness of emerging risks is therefore essential and can be supported through accessible training programmes, tailored informational resources and opportunities for dialogue with experts. Parental responsibility should not be understood as a set of prescriptive tasks, but as a practice of empathic mediation, where relational care becomes a prerequisite for building a home environment in which children can gradually exercise their right to exploration and experimentation. Parents are thus encouraged to play an active role not only in protecting their children but also in promoting autonomy and critical thinking. Recommended operational measures include: the development of accessible digital platforms supporting authoritative parenting practices, with modules on emotional intelligence, effective digital communication with adolescents and constructive intra-family dialogue; the provision of simple, user-friendly tools to activate parental controls at the time of purchase or registration (e.g. mandatory tutorials, intuitive interfaces, quick-start guides); the integration of proactive and easily usable functionalities (control panels, risk alerts, interactive tutorials, automated flagging

---

<sup>41</sup> See S. Leunig, E. Feldman, E. Schwartz, N. Dammasch, S. Brown, C. Miller, P. Sullivan, A. Mittal, *The Colorado AI Act: A Compliance Handshake Between Developers and Deployers*, 2025, available at: <https://mcusercontent.com/4edfeaee1cfab45c2f808237/files/9b99f02c-5a6a-771a-fadd-32907366d547/Colorado%20AI%20Act%20white%20paper.pdf>.

systems); the development of technologies that promote family digital safety, such as content filtering and monitoring applications, while also preserving children's evolving autonomy and privacy, in accordance with the child's age and maturity; and access to psychological support and counselling services for parents and children, coordinated with educational and healthcare services<sup>42</sup>.

Professionals working with children<sup>43</sup>, such as teachers, educators, psychologists, healthcare providers and social workers, occupy a key position in the construction of digital environments that are not only safe, but also developmentally appropriate and inclusive. In this capacity, they are called upon to act as reflective intermediaries between minors, families and technological systems. It is essential to integrate into continuous professional training topics such as digital citizenship, emotional intelligence, risk prevention and critical digital engagement, in order to promote a shared culture of digital well-being.

Beyond individual training, it is important also to promote the adoption of accessible and context-sensitive tools that enable professionals to guide children in navigating the digital world. These include intuitive control systems and didactic resources co-designed with children themselves, as well as digital platforms offering contextual guidance on emerging technologies. Specific features, such as "Educator controls" modelled on parental settings, can empower professionals to supervise educational platforms in ways that respect children's autonomy while ensuring appropriate safeguards.

Crucially, professionals are encouraged to facilitate open conversations with children about their online experiences, helping to bridge the divide between digital and offline life<sup>44</sup> and enabling the recognition of signs of emotional discomfort or distress. These practices are reinforced through collaborative initiatives involving families and social services, supported by practical tools such as short videos, intergenerational workshops and materials for use in school or home-based consultations. This approach finds solid grounding in the child's right to be heard, enshrined in Article

---

<sup>42</sup> CURA Blueprint Guidelines, *cit.*, pp. 5-8.

<sup>43</sup> *Ibidem*.

<sup>44</sup> On the topic, and with reference to the neologism "onlife" – describing the constant interpenetration of physical and digital realities – see L. Floridi, *La quarta rivoluzione. Come l'infosfera sta trasformando il mondo*, Milano, 2017.

12 of the UNCRC and widely affirmed in both European and Italian jurisprudence, which underscore the centrality of listening to the child as a prerequisite for meaningful protection and participation<sup>45</sup>.

Particular attention should be paid to the development of diagnostic and preventive tools capable of identifying adolescents who may be especially vulnerable to the emotional effects of AI-driven interactions. These tools, ideally designed in co-participation with children, should enable early and tailored interventions in cases of distress. Specialised training modules and certification programmes are also recommended, with a strong emphasis on emotional intelligence as a central component of digital safety. In line with this, the proposed approach underscores the need for professionals to be equipped to handle identity-sensitive issues, especially in the context of adoption, by supporting families in fostering emotionally aware and ethically grounded digital practices.

This multidimensional approach, combining technical, educational and emotional competences, resonates with the public strategies implemented in the UK and France, where the promotion of children's participation and the cultivation of digital resilience are recognised as essential pillars of digital governance.

Public and private organisations, particularly digital platforms and service providers are called upon to uphold principles of proactive responsibility and enhanced protection. Specific recommendations include: designing age-appropriate interfaces differentiated by age groups, using comprehensible language and layered functionalities; adopting transparent, updateable and interoperable systems for age verification and parental control; implementing accessible and responsive reporting mechanisms for minors and their caregivers, with immediate feedback and differentiated pathways based on age and exposure to risk; developing adaptive

---

<sup>45</sup> In the domestic legal framework, this orientation finds confirmation in the so-called *Cartabia Reform* (Legislative Decree n. 149 of 10 October 2022), implementing Delegated Law n. 206/2021. The reform introduced a far-reaching overhaul of civil procedure and of alternative dispute resolution mechanisms, with significant repercussions on proceedings concerning persons and family matters. Within this context, a more structured and detailed regulation of the child hearing procedure was established, designed to enhance not only the child's natural capacities and inclinations, but also his or her expectations and developmental aspirations. This approach emerges with particular clarity from the Explanatory Report to the decree, which expressly underscores the child's right to self-determination as an individual asset to be recognised and protected. See S. Rigazio, *L'Empowerment del minore nella dimensione digitale, cit.*, pp. 130 ff.

recommendation systems that avoid polarisation and stereotyping, tailoring content suggestions to children's cognitive and emotional development; and publicly disclosing the indicators used in risk assessment systems, as part of accessible transparency and monitoring reports. Active involvement of minors in service design, through co-creation processes, is strongly encouraged. These recommendations draw directly on the UK's Age-Appropriate Design Code, which introduced the first legally binding requirements for information society services targeting children, and which remains a key comparative reference for integrated online child protection<sup>46</sup>.

The active involvement of minors in shaping the strategies that affect their digital lives should be recognised as a central element of any child-centred regulatory framework. Emphasis should be placed on their participatory role and on the importance of developing tools that are genuinely responsive to their evolving needs. In this regard, particular value lies in the creation of child-friendly digital instruments<sup>47</sup>, designed according to usability and accessibility principles appropriate to different age groups and aimed at fostering emotional awareness, privacy protection and responsible online behaviour (such as educational avatars, gamified learning paths, narrative interfaces and alert notifications that encourage dialogue with trusted adults).

Children's participation is further supported through co-design workshops, focus groups and iterative feedback mechanisms<sup>48</sup>. In line with the BIK+ Strategy and best practices developed in France and the UK, this participatory approach is recognised as an effective form of empowerment. Crucially, however, it does not represent a sociological novelty but rather the continuation of a legal and regulatory trajectory already consolidated elsewhere. On the one hand, it follows the path traced by case law and international instruments, which have progressively emphasised the child's right to be heard and to be actively involved in decisions affecting them. On the other hand, it reflects broader regulatory trends in the digital economy, where experimentation and collaborative governance have increasingly been embraced as guiding principles. The analogy with the "regulatory sandbox" model is instructive: initially developed in the financial sector as a controlled environment in which

---

<sup>46</sup> CURA Blueprint Guidelines, *cit.*, pp. 3 – 4 – 7 - 8.

<sup>47</sup> Notably, even the Convention on the Rights of the Child itself has been made available in a child-friendly version, underscoring that accessibility and participation are not matters of sociology alone, but are firmly rooted in legal practice and principles.

<sup>48</sup> CURA Blueprint Guidelines, *cit.*, pp. 6 and 9.

innovative tools could be tested under light-touch supervision, this methodology has progressively spread to other domains of digital and AI governance<sup>49</sup>. In this perspective, children's involvement in shaping digital environments can be seen as part of the same experimental logic, a regulatory laboratory where rights, technologies and responsibilities are co-constructed through inclusive processes.

Listening to children and adolescents, valuing their digital expertise and recognising their concerns, means acknowledging them as active co-constructors of the digital world. In this sense, protection cannot be meaningfully separated from participation: one cannot truly protect those who are not included in the decisions that affect them.

Taken as a whole, the proposed framework reflects an integrated and multi-layered vision of child protection in digital environments, one that views vulnerability not as a fixed attribute, but as a dynamic and situated condition to be addressed through the careful balancing of safeguarding and the progressive development of autonomy. In this perspective, building truly child-friendly digital ecosystems requires moving beyond paternalistic approaches and embracing collective responsibility across all stakeholders.

Yet, the good practices outlined above are put to the test when vulnerabilities become more complex and interwoven, as in the case of adopted minors seeking information about their biological origins online. In such situations, standard protective frameworks may prove insufficient, calling instead for context-sensitive responses that combine legal safeguards with ethical guidance and emotional support. These more specific challenges are addressed in the following sections (5, 5.1 and 6), which focus on how vulnerability multiplies in adoption-related contexts and explore the corresponding need for targeted and ethically grounded policy interventions.

Then, a constant emphasis is placed on digital literacy and education as foundational dimensions, not only for fostering awareness and resilience, but also for enabling children's meaningful and informed participation in the digital sphere. While the present and following sections have primarily focused on the legal and technical pillars of intervention, Sections 7 and 8 provide a more in-depth discussion of educational practices from a comparative perspective. Section 9, in turn, offers concrete policy

---

<sup>49</sup> S. Rigazio, 'New techs, new threats': sfide e opportunità della rivoluzione blockchain, in *La cittadinanza europea Online*, 2021, pp. 61 ff.

recommendations relating to the educational pillar, understood as a key instrument for addressing and reconnecting the various layers of vulnerability through the large-scale promotion of digital awareness.

## **5. The complex balance between privacy preserving and search for origins**

As mentioned in the previous paragraphs, although childhood and adolescence are inherently associated with vulnerability, certain circumstances heighten this condition and call for targeted protective measures. The sensitivity of certain contexts is today further amplified by the potentialities of the digital environment, which can significantly impact already fragile family scenarios. Adoption represents one such context: the emotional and legal complexities surrounding identity and belonging render children particularly exposed, while digital technologies intensify this vulnerability by opening new, often risky, avenues for exploring their past and connections.

The case of adopted minors, specifically within the Italian legal framework, is particularly relevant for examining the balance between two different fundamental rights: on the one hand, the individual's right, including that of the minor, to know their origins, as an essential element in the construction of personal identity; on the other hand, the right to privacy during a safe navigation, which imposes limits on the access to, collection and dissemination of sensitive personal data, particularly in digital contexts. This requires a legal approach capable of reconciling self-determination with protection.

This analysis highlights the challenges in formulating legal solutions that can simultaneously safeguard the minor's need for truth and their exposure to digital risks, calling for an approach that is sensitive to context, age, and the vulnerability of the individual concerned.

The Italian legal framework on the search for origins is especially significant, as it reveals inconsistencies between the letter of the law, which grants only adult adoptees the right to undertake such a search, and actual practice, where even very young adoptees increasingly engage in this process, often leveraging digital technologies in a smart and intensive manner.

Following an overview of the legal framework governing origin tracing in Italy, the analysis will focus on the peculiarities of such a search when carried out online by a minor. Finally, the article will offer a comparative perspective, exploring how the search for origins is regulated in French and English legal systems, taking into account recent debates and the role played by new technologies in such jurisdictions.

Adopted minors are particularly vulnerable individuals, even when compared to their peers. They are often faced with the challenge of coming to terms with a difficult and obscure past, which compels them to question their biological origins and seek to discover the identity of their birth parents and relatives<sup>50</sup>. This process inevitably involves a highly emotional component, marking the search with unique features<sup>51</sup>.

Such considerations have led several countries to institutionalize this process by establishing dedicated mechanisms aimed at assisting adoptees in tracing their origins, while also safeguarding the privacy and rights of other individuals potentially involved. This is the case of Italy, which in its legislation on both domestic and international adoption, has included a specific provision addressing the situation of an adoptee who wishes to discover their origins, particularly the identity of the birth mother<sup>52</sup>. Specifically, the adoption law provides that adoptees over the age of twenty-five may submit a petition to the Juvenile Court of their place of residence in order to access information concerning their origins and the identity of their biological parents<sup>53</sup>.

A notable peculiarity of the procedure lies in the age requirement set by the legislature: the threshold of 25 years substantially exceeds the legal age of majority in Italy, set at

---

<sup>50</sup> M. D. Schechter, D. Bertocci, *The meaning of the search. The psychology of adoption*, New York, NY, US: Oxford University Press, 1990; W. Tieman, J. van der Ende, F. C. Verhulst, *Young adult international adoptees' search for birth parents*, in *Journal of Family Psychology*, 2008.

<sup>51</sup> R. Rosnati, R. Iafrate, *Psicologia dell'adozione e dell'affido familiare*, Vita e Pensiero, Milano, 2023, pp. 206 ff.; D.M. Brodzinsky, M.D., Schechter, R. Marantz Henig, *Being adopted. The lifelong search for self anchor*, New York: Books Ed., 1993.

<sup>52</sup> L. n. 184/1983, the Italian adoption law, entitled “*Diritto del minore a una famiglia (Child's right to a family)*”.

<sup>53</sup> Article 28, par. 5 and 6. The same article provides for exceptions regarding the age threshold where particular conditions exist: 18 years if there are serious and proven reasons relating to the psycho-physical health of the adopted child while, in the case of serious and proven reasons, such a request can be made directly by the adoptive parents of the minor. This is, in any case, a delicate procedure, involving hearings of individuals deemed necessary by the Court, and, more importantly, a psychosocial assessment of the applicant. The aim is to prevent such disclosure from excessively disturbing the applicant's psychological well-being.

18, when an individual is already legally entitled to make independent decisions and manage their own interests<sup>54</sup>.

Nonetheless, the most distinctive aspect of the Italian legal framework is found in another provision: the so-called "anonymous birth" (*parto anonimo*), which establishes that access to the requested information is not permitted if the birth mother, at the time of delivery, declared her wish not to be identified<sup>55</sup>. According to the letter of the law, such a declaration entails an absolute and irreversible prohibition for the adoptee to initiate any procedure to discover the birth mother's identity<sup>56</sup>.

Within the European context, Italy stands as a significant exception. In addition to Italy, only France and Luxembourg provide for anonymous birth, granting pregnant women the option to remain unidentified<sup>57</sup>. In contrast, most of the EU Member States do not recognise this possibility, giving priority to the principle of automatic maternal recognition. In these jurisdictions, anonymous birth is prohibited to ensure that the child's right to know their origins is always preserved<sup>58</sup>.

---

<sup>54</sup> Upon reaching adulthood, individuals are generally granted access to most private and public rights, including employment and voting. For an overview of the legal capacity of minors within the Italian legal system: F.D. Busnelli, *Capacità ed incapacità di agire del minore*, in *Diritto di famiglia e delle persone*, Milano, 1982, pp. 54 ff.; F. Giardina, *La condizione giuridica del minore*, Napoli, 1984.

<sup>55</sup> This is possible pursuant to Article 30, paragraph 1, of Presidential Decree n. 396 of 3 November 2000, which states: "The birth declaration is made by one of the parents, by a special proxy, or by the doctor or midwife or other person who attended the birth, respecting the mother's wishes not to be named".

<sup>56</sup> The rationale behind this provision is rooted in the legislature's intent to prevent abortion and infanticide by allowing for safe deliveries and avoiding dangerous abandonment. At its core lies the protection of the right to life of both the mother and the newborn. However, the law also aims to safeguard additional rights, including health, privacy, personal autonomy, and the right to be forgotten: E. De Belvis, *Il diritto dell'adoottato di conoscere le proprie origini biologiche*, in *Fam. Dir.*, n. 10, 2017, pp. 396 ff.; G. Casaburi, *Il parto anonimo dalla ruota degli esposti al diritto alla conoscenza delle origini*, in *Foro it.*, n. 1, 2014, pp. 8 ff.; V. Marcenò, *Quando da un dispositivo d'incostituzionalità possono derivare incertezze*, in *Nuov. Giur. civ. comm.*, n. 4, 2014, pp. 279 ff.

<sup>57</sup> For an overview in legal European field: L. Balestra, E. Bolondi, *La filiazione nel contesto europeo*, in *Fam. Dir.*, n. 3, 2008, pp. 310 ff.; B. Knoll, *Il diritto al parto in anonimato*, in *Milan Law Review*, v. 3, n. 1, 2022, pp. 100 ff.; E. Andreola, *Fratelli biologici di madre anonima e riservatezza dei dati genetici*, in *Fam. Dir.*, n. 3, 2020, pp. 281 ff.; Outside the strictly EU area, Russia and Slovakia, in accordance with Italian, Luxembourg, and French law, provide for anonymous birth. For a comparison with English and French law, see the next section.

<sup>58</sup> Specifically, Spain initially allowed anonymous births, which was declared unconstitutional in 1999 by the Supreme Court: B. Grazzini, *Diritto alla conoscenza delle proprie origini e riservatezza nei rapporti di filiazione*, Aracne, Roma, 2018, pp. 47 ff. Other countries that prioritize maternity certification include England, the Netherlands, Portugal, Belgium and Denmark.

Between these two regulatory models lies a third: the Germanic legal systems. Germany and Switzerland, long-time advocates of the right to origin disclosure, have recently introduced the institution of "confidential birth" (*vertrauliche Geburt*), which constitutes a moderated approach to the previously absolute nature of the right to biological identity<sup>59</sup>.

Until the last decade, the Italian framework was extremely rigid, admitting no exceptions or derogations and establishing the mother's anonymity as an unchallengeable principle. It took judicial intervention - both domestic and supranational - to soften the rigidity of the institution<sup>60</sup>.

Over time, awareness has grown regarding the importance for adoptees of knowing their origins as part of the process of constructing their individual and psychological identity<sup>61</sup>. This aligns with the principle of the best interest of the child, which encompasses the right of the grown child to understand their own past<sup>62</sup>. This has led to the introduction of the so-called *interpello* procedure, a legal mechanism that partially recognises the right of the adoptee to know their origins.

The *interpello* allows the Court to contact the birth mother and give her the opportunity - if she so wishes - to revoke the anonymity declared at the time of birth. If the mother consents, the adoptee gains access to her identifying information. If not, her identity remains protected.

---

<sup>59</sup> On the German legal system: C. Rusconi, *La legge tedesca sulla vertrauliche Geburt. Al crociera tra accertamento della maternità, parto anonimo e adozione*, in *Eur. Dir. priv.*, n. 4, 2018, pp. 1347 ff. Regarding the Swiss legal system, however, please consult the Rapporto del Consiglio federale in adempimento del postulato Maury Pasquier 13.4189 "Migliorare il sostegno alle madri in difficoltà e alle famiglie vulnerabili", 12 December 2013, 12 October 2016, available on [www.admin.ch](http://www.admin.ch).

<sup>60</sup> M.N. Bugetti, *Parto anonimo: la secretazione dell'identità della madre si protrae anche dopo la sua morte*, in *Fam. Dir.*, n. 12, 2020, pp. 1140 ff. and, the same author, *Il diritto all'anonimato della madre incapace prevale sul diritto del figlio a conoscere le proprie origini*, in *Fam. Dir.*, n. 7, 2021, pp. 748 ff.

<sup>61</sup> G.M. Wrobel, H.D. Grotevant, *Minding the (information) gap: what do emerging adult adoptees want to know about their birth parents?*, in *Adoption Quarterly*, 22(1), 2019, pp. 29 ff.; A.Y. Kim, O.M. Kim, A.W. Hu, J.S. Oh, R.M. Lee, *Conceptualization and measurement of birth family thoughts for adolescents and adults adopted transnationally*, in *Journal of Family Psychology*, 34(5), 2020, pp. 555 ff.; F. Vadilonga, *Curare l'adozione*, Milano, Raffaello Cortina, 2010.

<sup>62</sup> United Nations Committee on the Rights of the Child (2013). General comment n. 14 (2013) on the Right of the Child to Have His or Her Best Interests Taken as a primary consideration, CRC/C/GC/14. <https://www.refworld.org/docid/51a84b5e4.html>; Z. Vaghri, R. Ruggiero, G. Lansdown, *Children's Rights-Based Indicators. Strengthening States' Accountability to Children*, Springer, 2025.

The introduction of this institution was made possible by the intervention of the Italian Constitutional Court, which declared unconstitutional the provision of the Adoption Law insofar as it did not allow the biological mother to revoke her anonymity, and urged the legislator to enact legislation on the matter<sup>63</sup>.

Despite the Constitutional Court's explicit call, no implementing legislation has been enacted since 2013. In the absence of statutory regulation, the Juvenile Courts have been *de facto* entrusted with managing this delicate issue. As a result, diverse and often inconsistent judicial practices have emerged, which the Court of Cassation has occasionally attempted to standardise<sup>64</sup>.

Furthermore, the courts are now faced also with increasingly complex and unforeseen scenarios. These have led to the development of additional judicial interpretations, including: the right to know the identity of a deceased mother; the inadmissibility of the *interpello* in cases where the birth mother is still alive but legally incapacitated; and the possibility of identifying biological siblings<sup>65</sup>.

Therefore, the legal possibility of giving birth anonymously and of searching for one's origins is currently governed by a limited number of legislative provisions and a few, but fundamental, rulings from the highest Italian courts.

Despite the active role played by the Constitutional and Supreme Courts, the *interpello* procedure still suffers from a significant legislative gap<sup>66</sup>. This lack of legislation

---

<sup>63</sup> Godelli v. Italy, HUDOC, 25 September 2012, appeal n. 33783/09. V. Carbone, *Corte Edu: conflitto tra diritto della madre all'anonymato e diritto del figlio a conoscere le proprie origini*, in *Corr. giur.*, n. 7, 2013, pp. 960 ff.; G. Currò, *Diritti della madre all'anonymato e diritto del figlio alla conoscenza delle proprie origini. Verso nuove forme di contemporamento*, in *Fam. Dir.*, n. 6, 2013, pp. 537 ff.; A. Margaria, *Parto anonimo e accesso alle origini: la Corte europea dei diritti dell'uomo condanna la legge italiana*, in *Min. Giust.*, n. 2, 2013, pp. 340 ff.; D. Butturini, *La pretesa a conoscere le proprie origini come espressione del diritto al rispetto della vita privata*, in *Forum di quaderni costituzionali*, 24 October 2012, pp. 1 ff.

<sup>64</sup> The Supreme Court of Cassation provided an overview of the practices adopted by various Italian Juvenile Courts, accounting for the differences and commonalities that characterize the *Interpello* procedure, in its Joint Sections ruling n. 1946 of January 25, 2017.

<sup>65</sup> These rulings were reached in Supreme Court rulings n. 15024 of July 21, 2016, n. 7093 of March 3, 2022, and n. 6963 of March 20, 2018.

<sup>66</sup> Over the years, several legislative proposals have been advanced, yet none has been enacted into law. The last two, dating back to the previous legislature, are: S. n. 1039, Provisions regarding social welfare services, anonymous births, and access to information on the origins of a child not recognized at birth, initiated by the Hon. Giuseppe Luigi Salvatore Cucca (Pd) and others, 31 January 2019, last discussed on 6 July 2022; S. n. 922, Provisions regarding the right to know one's biological origins, initiated by the Hon. Simone Pillon and F. Urraro (L.-Sp.-Psd'Az.) 7 November 2018, also last discussed on 6 July 2022.

undoubtedly jeopardises the right of adoptees to investigate their roots, a right that remains dependent solely on judicial interpretation. Furthermore, new challenges are emerging in the field of adoption, closely linked to the issues of origin tracing and the *interpello* procedure.

First, it is increasingly likely that in the near future, adoptees will seek to identify not only their birth mothers and siblings but also other biological relatives, such as fathers, grandparents, and uncles or aunts.

Second, it is likely that one of the most pressing issues on the horizon is the right of children born through heterologous assisted reproduction or international surrogacy to discover their origins<sup>67</sup>.

Finally, there is the issue that concerns all adopted individuals: the possibility of tracing their origins via the internet, bypassing institutional channels and in the absence of a clear regulatory framework defining its limits, methods, and ethical implications. This exposes them, as minors, to a range of risks and opportunities that are inherent to online navigation and deserve careful examination<sup>68</sup>. For this reason, it is essential that children and adolescents are adequately equipped to understand and recognise the dynamics of the digital environment, enabling them to navigate it with greater awareness and autonomy, particularly given its significance in the construction of personal identity. Such preparation necessarily involves a process of digital literacy aimed at developing critical skills and discernment, thereby promoting safe and informed use of online tools.

To this end, it is useful to examine how the issue of origin tracing has been addressed in other legal systems. A comparative analysis of normative frameworks, judicial approaches, and administrative practices may offer valuable insights and reflections for the development of more balanced and child-friendly models of intervention, capable of integrating the right to know one's origins with the need for protection, privacy, and appropriate support throughout the digital search process.

---

<sup>67</sup> V. De Santis, *Diritto a conoscere le proprie origini come aspetto della relazione materna. adozione, pma eterologa e cognome materno*, in *Nomos. Le attualità di diritto - Quadrimestrale di teoria generale, diritto pubblico comparato e storia costituzionale*, 2018, pp. 1 ff.

<sup>68</sup> See paragraph 6.

### 5.1 Towards a responsible approach: lessons learnt from the French and UK systems

Continuing from the previous paragraphs, a comparative analysis was carried out on the issue of origin tracing in the legal systems of France and UK. This choice is motivated by several factors.

As far as the French legal system is concerned, various elements must be considered. Firstly, French law shares with Italian law the same historical roots of the adoption institution, both being grounded in the Roman law tradition<sup>69</sup>. Furthermore, with specific regard to the right to origins, France has played a pioneering role in influencing the Italian legal debate<sup>70</sup>. Finally, in terms of the solutions adopted, the French legal framework has opted for a model that significantly diverges from the Italian one.

As for the UK legal system, the comparative interest stems from different considerations, primarily related to the fact that the two countries exhibit profoundly different legal and cultural traditions in the field of adoption. This divergence is reflected in the legal practices and regulations governing access to personal and biological origin information for adopted children, laying the foundation for different approaches to autonomous searches via the internet. These differences mirror distinct conceptions of the right to identity and the protection of the individuals involved.

All these aspects may provide valuable insights for the Italian legal system, which appears to be “caught” in an unresolved situation requiring prompt and well-structured solutions. The first steps in this direction must necessarily include a long-overdue process of digital literacy, which should engage all segments of society, albeit to varying degrees, with the aim of genuinely implementing the principle of the best interest of the child, including within the digital environment.

---

<sup>69</sup> J. Long, *Uno sguardo altrove: l'adozione dei minorenni in Francia, Inghilterra e Spagna*, in *Min. Giust.*, n. 4, 2017, pp. 132 ff.

<sup>70</sup> A. Renda, *La sentenza Odièvre c. Francia della Corte Europea dei diritti dell'uomo: un passo indietro rispetto all'interesse a conoscere le proprie origini biologiche*, in *Familia*, n. 6, 2004, pp. 1109 ff.; A. O. Cozzi, *La Corte costituzionale e il diritto di conoscere le proprie origini in caso di parto anonimo: un bilanciamento diverso da quello della Corte europea dei diritti dell'uomo?*, in *Giur. Cost.*, n. 6, 2005, pp. 4609 ff.; D. Paris, *Parto anonimo e bilanciamento degli interessi nella giurisprudenza della Corte costituzionale, del Conseil constitutionnel e della Corte europea dei diritti dell'uomo*, in *Forum di Quaderni costituzionali*, n. 10, 2012, pp. 447 ff.

The French legal system shares with the Italian one the historical and legal foundations that led to the current institution of adoption, governed by Articles 343 ff. of the *Code Civil*. Notably, France is one of the few European countries to allow anonymous childbirth (*accouchement sous X*), introduced to safeguard the life and health of both mother and child<sup>71</sup>. Moreover, France has historically served - and continues to serve, as a model for the Italian legal system with regard to the *interpello* procedure (i.e. the process of contacting the birth mother to seek her consent to disclose her identity), which was directly inspired by the French experience<sup>72</sup>.

Since 2002, French law has allowed that, notwithstanding the mother's right to give birth anonymously, the child may later request access to information about their origins, subject to the biological mother's consent to waive anonymity<sup>73</sup>.

Specifically, this process is facilitated by a dedicated body, the *Conseil National pour l'Accès aux Origines Personnelles* (CNAOP), established within the Ministry of Social Affairs. This body acts as an intermediary: it receives requests from adoptees and attempts to contact the birth mother; if consent is granted, it enables contact between the two parties<sup>74</sup>.

This legal mechanism attracted scholarly attention in 2003 when it was brought before the European Court of Human Rights in the landmark case *Odièvre v. France*<sup>75</sup>. In that decision, the Court upheld the compatibility of the French system with Article 8 of

---

<sup>71</sup> A woman's right to give birth anonymously is provided for both in the *Code de l'action sociale et des familles* (Articles L.222-6 and L.224-5, as amended by Law n. 2002-93 of 22.1.2002) and in the *Code civil* (Articles 341 and 341-1, as amended by Law 93-22 of 8.1.1993).

<sup>72</sup> N. Falbo, *Il diritto alle origini fra ordinamenti nazionali e giurisprudenza europea. Spunti per una comparazione*, in *Diritti fondamentali.it*, n. 2, 2020, pp. 1060 ff.

<sup>73</sup> L. 2002-92 del 22.1.2002. F. Bellivier, *Accès aux origines. Loi No .2002-92 du 22 janvier 2002 relative à l'accès aux origines des personnes adoptées et pupille de l'Etat*; B. Mallet-Bricout, *Réforme de l'accouchement sous X: quel équilibre entre les droits de l'enfant et le droit de la mère biologique?*, in *JCP*, 2002, pp. 119 ff.

<sup>74</sup> J. Long, *La corte europea dei diritti dell'uomo, il parto anonimo e l'accesso alle informazioni sulle proprie origini: il caso Odièvre c. Francia*, in *Nuov. Giur. Civ. Comm.*, n. 2, 2004, pp. 295 ff.

<sup>75</sup> This is the ruling issued on 13 February 2003, appeal n. 42336/1998. F. Rivero Hernández, *De nuevo sobre el derecho a conocer el propio origen. El asunto Odièvre (sentencia del Tribunal Europeo de Derechos Humanos de 13 de febrero de 2003)*, in *Actualidad Civil*, 2003, pp. 593 ff.; L. Rodríguez Vega, *Los límites del derecho a conocer la propia identidad. Comentario a la sentencia del tribunal europeo de derechos humanos de 13-2-2003, caso Odièvre contra Francia (TEDH 2003, 8)*, in *Repertorio Aranzadi del Tribunal Constitucional*, 2003, n. 4, Parte Estudio.

the European Convention on Human Rights, laying the groundwork for subsequent Italian jurisprudential developments.

Although the Italian *interpello* procedure is explicitly inspired by the French model, significant and evident differences remain. First, the French approach is codified in statutory law, whereas Italy still lacks specific legislative intervention, despite long-standing academic and institutional calls for reform. Second, the Italian procedure is entirely judicial in nature, while the French CNAOP operates as an administrative (non-judicial) body. This latter structure is arguably more suitable to perform the mediating role assigned to it by law.

In the context of origin tracing conducted online, the structure of the CNAOP lends itself more readily to integration with the measures outlined in the next paragraph. Its centralised, institutional design is well-suited to balance the right to know one's origins with the privacy rights of those involved. The integration of secure digital tools, identity verification procedures, and protected communication platforms could further enhance its effectiveness, ensuring personalised support, respect for fundamental rights, and greater protection against the risks of indiscriminate use of online platforms.

Digital literacy initiatives could also acquire a more systemic scope if coordinated by a dedicated body capable of addressing the needs of all actors involved: minors, adoptive families, social workers, and institutions. A coordinated, multidisciplinary effort by a specialised unit could develop shared guidelines, provide differentiated and up-to-date training programmes, and design educational tools tailored to different age groups and vulnerabilities. This would strengthen minors' ability to navigate the digital environment in a conscious and safe manner.

With regard to the UK legal system, it is based on entirely different premises<sup>76</sup>. Unlike France and Italy, UK belongs to the group of jurisdictions that automatically recognise parental relationships at birth and do not provide for anonymous childbirth. Under this legal framework, adopted individuals who reach the age of majority may request access to the information contained in their personal file from the competent

---

<sup>76</sup> The legal framework is broadly similar regarding the legislation in the UK, Wales, Scotland, and Northern Ireland. Specifically, adoption is governed in England and Wales by the Adoption and Children Act 2002; in Scotland by the Adoption and Children (Scotland) Act 2007; and in Northern Ireland by the Adoption (Northern Ireland) Order 1987.

court and the adoption agency. If such information is subject to confidentiality restrictions, the agency has a margin of discretion and must weigh the adopted person's interest against other competing rights and circumstances of the individual case.

To facilitate this, the *Adoption Contact Register* was established<sup>77</sup>, allowing adult adoptees, their siblings, and other members of their birth families to express their interest in re-establishing contact with relatives from whom they have been separated. Access to information is granted only where there is a match between registered requests, based on a logic of reciprocity and voluntary contact<sup>78</sup>.

As in the French experience, and unlike the Italian model, the English system for accessing origins is structured and governed by legislative provisions, rather than left to judicial interpretation and case law. However, unlike France, UK has opted for a system based on registries and databases, rather than a centralised administrative authority.

Following this approach, the UK has also begun to reflect on origin tracing in the context of medically assisted reproduction (MAR<sup>79</sup>). In this area, the *Donor Conceived Register* and the *Donor Sibling Link* have been established to facilitate, within legal limits, access to information about donors and potential genetic siblings. These tools extend the principle of transparency to non-adoptive but medically assisted forms of parentage<sup>80</sup>.

In both legal contexts, however, the issue arises previously discussed of minors seeking information about their genetic past through digital tools and online platforms.

---

<sup>77</sup> Available at <https://www.gov.uk/adoption-records>. In Scotland, the relevant bodies are National Records of Scotland (<https://www.nrscotland.gov.uk/>) and Birthlinks (<https://birthlink.org.uk/>); Northern Ireland has its own Adoption Contact Register (<https://www.nidirect.gov.uk/articles/tracing-and-contacting-birth-relatives-and-adopted-adults#toc-4>).

<sup>78</sup> O. Faranda, *Il mantenimento della memoria dei bambini adottati nell'esperienza anglosassone*, in *Min. Giust.*, n. 1, 2017, pp 116 ff.

<sup>79</sup> Known also as assisted reproductive technology (ART).

<sup>80</sup> R. Hertz, *The Importance of Donor Siblings to Teens and Young Adults: Who Are We to One Another?*, in F. Kelly, Dempsey D, Byrt A, (eds). *Donor-Linked Families in the Digital Age: Relatedness and Regulation*, Cambridge University Press, 2023.

England has undoubtedly adopted a more structured approach to ensuring the safety of minors online, but it is not exempt from the safeguards and recommendations outlined above. Despite its institutionalised and regulatory framework for digital safety, the UK system still requires complementary educational measures, support mechanisms, and operational practices to guide minors in a safe, informed, and rights-respecting journey of origin tracing.

Across all three legal contexts examined, there is a clear need to complement the normative frameworks, albeit differing in structure and foundation, with measures that ensure a safe and informed support system for the search for origins conducted through digital means. Within this framework, the promotion of digital literacy plays a central role: adequate digital education is essential to enable minors to navigate the online environment, understand the implications of their choices, recognize potential risks, and protect themselves as well as other parties involved. Secure digital environments and tailored educational pathways should be integrated within a coordinated and multidisciplinary institutional approach. Such a systemic intervention can effectively balance the right to identity and knowledge of one's origins with the safety and protection of all individuals concerned.

## **6. Search for origin on digital environment: take away recommendations**

The Italian legal system, as has been noted, establishes a judicial procedure enabling adopted individuals to initiate research into their origins only once they reach the age of twenty-five. In practice, however, a different reality emerges: many adopted minors pursue information about their biological families through the internet well before reaching that age.

This discrepancy is unsurprising: on one hand, there is the statutory age threshold required by law; on the other, the now-established practice of promptly informing the child of their adoptive status<sup>81</sup>. With such awareness, a desire to explore one's past may arise early on. The internet is the most immediate, convenient, and cost-free medium to commence such an inquiry.

---

<sup>81</sup> Furthermore, Article 28, paragraph 1 of Law 184/1983 provides that "*the adopted minor is informed of his or her condition and the adoptive parents shall provide for this in the ways and within the terms they deem most appropriate*".

Certainly, the wealth of online information, the ease of device usage, and the speed of browsing encourage children and adolescents to pursue their origins domestically. The variety of devices, smartphones, tablets, personal computers, further facilitates autonomous research by young users<sup>82</sup>.

Moreover, widespread use of social media provides unprecedented opportunities for connection, expanding how one may come into contact with biological relatives. Although young people often display apparent proficiency in digital environments, they frequently navigate the web unaware of inherent risks and the behavioural dynamics of social platforms. The term “digital natives” may be misleading: being immersed in digital media does not automatically equip minors with appropriate technological competence, especially when their adoptive status might compromise the cautiousness normally expected in online activity<sup>83</sup>.

As explored above, the digital environment presents numerous opportunities and risks for minors. In the case of adopted minors, the impact is more significant, particularly absent adequate digital literacy. Nonetheless, multiple and varied benefits should not be overlooked or dismissed.

First and foremost is access to knowledge of one’s cultural and geographical roots, whether in international adoptions (outside Italy) or domestic ones (adoption across regions within Italy), which supports the development of personal identity. Likewise, connecting with peers facing similar experiences can be beneficial: healthy peer interaction and shared experiences may reduce the isolation and distress often felt by adopted individuals.

In general, origin-related research can serve as an educational opportunity, stimulating interests in history, geography, or the language of the country of origin, and fostering

---

<sup>82</sup> G. Mascheroni, A. Cuman, *Net Children Go Mobile: Final Report*, Educatt, Milano, 2014; G. Mascheroni, K. Ólafsson, *Net Children Go Mobile: risks and opportunities. Second edition*, Milano: Educatt, 2014; C. Garitaonandia; I. Karrera, N. Larrañaga, *Media convergence, risk and harm to children online*, in *Doxa Comunicación*, n. 28, 2019, pp. 179 ff.

<sup>83</sup> M. Prenksy, *Listen to the Natives*, in *Educational Leadership*, v. 63, n. 4, 2005, pp. 8 ff.; A. Guarini, *S.M.E.N., Internet e social: i ragazzi raccontano le possibilità e i rischi della rete*, in *I Quaderni dell’Ufficio Scolastico Regionale per l’Emilia Romagna*, 2018, pp. 61 ff.; M. Martoni, *Datificazione dei nativi digitali. Una prima ricognizione e alcune brevi note sull’educazione alla cittadinanza digitale*, in *Federalismi.it*, 8 January 2020.

digital, cultural, and relational competencies, thus empowering the individual<sup>84</sup>. Additionally, autonomous research allows the minor to choose the pace and mode of inquiry, aligning with their emotional rhythm and cultivating self-awareness of needs, desires, and curiosity.

Another positive dimension of such online research is access to legal resources: the minor can gain information about their rights as an adopted individual, the protections available, and the instruments designed specifically with origin-search procedures in mind<sup>85</sup>.

These advantages are counterbalanced by a similarly extensive array of risks to which adopted minors, experienced web users, children or adolescents, are exposed when conducting origin research via digital devices.

Impulsivity, a characteristic common in youth, coupled with the powerful desire to reconstruct one's personal history, renders adopted minors particularly vulnerable to digital risks, amplifying their consequences. Typical online hazards, such as privacy breaches, exposure of personal or non-personal data, grooming, emotional manipulation, fraud, identity theft, and scams, take on heightened significance.

Specifically, the emotional intensity of origin searches may lead the minor to initiate and sustain contact with strangers whom they might otherwise distrust, contravening basic safety guidelines. Even prudent behaviour during the inquiry cannot eliminate significant risks: children and adolescents may still encounter misinformation or harmful content that can profoundly affect identity formation.

Furthermore, even when research yields tangible results, minors may not be psychologically prepared to process those outcomes, which could provoke emotionally destabilizing or even traumatic effects, especially absent adequate psychological support. When such research is conducted autonomously or clandestinely, without adult awareness or guidance, it becomes difficult to manage potentially life-altering revelations.

---

<sup>84</sup> G. Martínez, M. Garmendia, C. Garitaonandia, *La infancia y la adolescencia ante las Tecnologías de la Información y la Comunicación (TIC): oportunidades, riesgos y daño*, in *Zer*, 25(48), 2020, pp. 349 ff.

<sup>85</sup> M. Casonato, *Adolescenti "in rete": navigare alla ricerca delle proprie origini*, in *Min. Giust.*, n. 4, 2015.

The modalities of origin research online vary. Some minors may post announcements on dedicated websites, though many of these platforms are unsuitable for minors, containing advertisements, donation requests, or product sales<sup>86</sup>. Certain sites offer DNA testing kits for purchase, often promising access to census records, passenger lists, or birth registries in exchange for payment<sup>87</sup>.

Social media usage is the most common method for locating biological relatives: through dedicated Facebook groups, specialized hashtags, or personal reels recounting one's story, sharing photos or documents, and appealing to the internet community. Such practices sacrifice basic safety measures: they frequently compromise privacy and encourage sharing information with anyone who expresses interest.

Similarly, there are online services offering accompaniment for origin searches in the adoptee's country of origin. Many of these services lack official certification or guarantees of professionalism, transparency, and reliability<sup>88</sup>. Often, they advertise the possibility of direct contact between the adoptee and a found relative without psychological or legal mediation. This exposes minors to significant emotional, safety, and rights-related risks, particularly when the desire to reconnect intersects with fragile expectations and deep emotional needs.

Moreover, beyond scenarios where the adoptee initiates research, it is increasingly common for biological relatives to search for and contact the minor via digital means. In the social media era and with widespread sharing of personal information, unexpected contact can lead to complex and potentially invasive dynamics. It is therefore essential to prepare adopted minors to handle unsolicited contact, including from biological family, through digital literacy and protection of their private sphere, to safeguard their psychological well-being and security.

---

<sup>86</sup> B. Bertetti, *Adottivi italiani alla ricerca delle origini: voci dal web*, in *Min. Giust.*, 2013, n. 2, pp. 203 ff.

<sup>87</sup> Suffice it to say that the website Ancestry.it promises to reconstruct your family tree for 199 euros a year, offering "access to over 20 billion historical documents from Italy and around the world".

<sup>88</sup> There are certainly valid services: Ser.I.O. is an Italian service that provides comprehensive assistance in the search for origins but scrupulously adheres to the age limits required by law. The results can be consulted at M. Parente, L. Ricciardi, *Centro Regionale di documentazione e ricerca per l'infanzia e l'adolescenza, La ricerca delle informazioni sulle origini. Riflessioni sulla complessità dei processi e proposte per un percorso condiviso*, 2022, Istituto degli Innocenti, Firenze; The same can be said for Radici Russe, based in France, whose activity is visible on <https://russianroots.org/en/achievements/>.

Considering these dynamics, integrating robust digital literacy initiatives into adoption support pathways is essential.

Equipping minors with tools to navigate the digital environment consciously involves not only imparting technical skills but primarily educating them to recognise risks, protect their online identity, and critically assess information and contacts, including those originating from their familial background. Digital literacy functions here as a cornerstone of self-determination, security, and emotional safeguarding within an increasingly complex and permeable online ecosystem. Furthermore, against this background, it serves as a practical tool for achieving the child's best interests, as required by national and international regulations.

Based on these considerations, practical recommendations grounded in a children's rights-based approach may be directed to multiple stakeholders: legislators; social services; businesses; professionals (educators, psychologists); minors; and parents<sup>89</sup>.

The first set of recommendations concerns the legislator, who bears the urgent and inescapable responsibility of developing a modern, child-centered legislative framework, capable of responding to the pressing contemporary relevance of the issue.

First and foremost, it is necessary to follow up on Constitutional Court judgment by introducing the formal request mechanism (so-called *interpello*), which has already been validated through the consolidated practice of Italian courts. However, such legislative action should not merely comply with the Court's recommendations but should instead take into account - and adapt to - the realities of the digital environment, while at the same time ensuring the full spectrum of safeguards that children currently require, including the protection of privacy, identity, and the right to be heard.

On one hand, it would be appropriate to reconsider the minimum age requirement for access to the origin-search procedure currently established by Italian law. On the other hand, it is essential to address the growing phenomenon of online origin searches, by acknowledging the associated risks and the potential impact on minors involved. This includes a thorough evaluation of the implications of digital

---

<sup>89</sup> For the specific set of policy recommendations targeting young adoptees, see *CUR4 Blueprint Guidelines, id.*, pp. 14-8.

technologies and artificial intelligence algorithms, particularly regarding their role in facilitating unauthorized or unexpected contacts between adopted minors and their biological relatives.

Therefore, the law itself should also reinforce the capacity of social services to implement psychological support programs for those minors who express the need to inquire into their biological origins.

Moreover, it would be desirable to establish a clear procedure for conducting origin searches even in cases of international adoption, taking full advantage of the unprecedented opportunities offered by the web<sup>90</sup>. In addition, another area where legislative intervention would be appropriate concerns the establishment of an institutional, public, free-of-charge, and specialized service to mediate origin searches, available to individuals who wish to make use of such support<sup>91</sup>.

More broadly, there is a compelling need to promote policies that require digital platforms to adopt specific measures aimed at recognizing and mitigating the potential emotional harm caused by the repeated and automated exposure to adoption-related content and narratives.

Given the importance that social services play in the field of pre- and post-adoption, being called to accompany the family unit that has embarked on the path of adoption so that the best interest of the child is guaranteed, some recommendations must also be made with respect to them.

These are measures designed with the objective of creating a specialized sector within the public service, focused on the needs of adopted minors, equipped to manage origin searches, including those conducted online, and active throughout the national territory.

Certainly, it is of primary importance to rethink university education in Social Work, strengthening academic programs in order to better prepare future professionals for

---

<sup>90</sup> Currently, the origins search is only available for national adoptions, not international ones. Despite this, the number of applications from international adoptees is increasing: R. Romano, *Parto anonimo e interpello: considerazioni alla luce di uno studio sulle prassi in uso presso il Tribunale per i Minorenni di Trento*, in Fam. Dir., n. 7, 2024, pp. 709 ff.

<sup>91</sup> Similar to the French CNAOP: see previous section.

the complexities of contemporary social challenges<sup>92</sup>. Still on the academic level, it is fundamentally important to invest in research on the well-being of minors, allocating resources to studies that guide evidence-based practices and policy development in the sector<sup>93</sup>.

Similarly, coordination among territorial social services is desirable, establishing collaboration mechanisms to harmonize practices and share best approaches. This would facilitate the implementation of uniform procedures at the national level, as well as the standardization of processes among regions, to ensure fair provision of services and protect the rights of minors throughout the country.

The guarantee of consistency and quality in social services should also be ensured through the publication of guidelines and the dissemination of standardized protocols<sup>94</sup>.

With regard to the focus on the online search for origins, the development of specialized training programs and guidelines for social workers is necessary, focusing on digital literacy, emotional intelligence, and understanding of the risks related to algorithms.

This with the aim of preparing them to effectively support adopted minors and families in managing emotional distress and unexpected online encounters with biological relatives.

Finally, the drafting of psychological support protocols specifically addressing digital vulnerabilities and emotional triggers specific to adopted minors conducting online searches on their biological origins would also constitute a valuable operational tool.

---

<sup>92</sup> Indeed, it's the Social Work's code of ethics itself that establishes in the preamble that "*Social workers are required to systematically improve their knowledge and skills through processes of constant debate, training, and self-reflection, to ensure the proper practice of the profession*" (on chrome-extension://efaidnbmnnibpcajpcgclefindmkaj/https://cnoas.org/wp-content/uploads/2020/03/Il-nuovo-codice-deontologico-dellassistente-sociale.pdf).

<sup>93</sup> As suggested by A. Bartolomei, E. Tognaccini, *Il diritto del minore agli interventi necessari: affidamento solidaristico e/o al servizio sociale (d.l. n. 149 art. 5-bis)*, in Min. Giust., n. 2, 2022, pp. 34 ff.

<sup>94</sup> A. Bartolomei, E. Tognaccini, *cit.*

Regarding the category of economic operators, the aim is to establish a series of safety measures to make platforms safer for adopted minors engaged in the search for their origins.

First and foremost, the mandatory integration of privacy by design and by default, as required under Article 25 GDPR, should be ensured in the design of digital products and services, adapted to the possible vulnerabilities of users.

Also the regular conduction of audits and vulnerability assessments, on the one hand, and the drafting of reporting and response protocols for security incidents, on the other, would be part of a strategy aimed at making the activities of economic operators more child-friendly, in line with the obligations set out in the DSA (Art. 34 ff.) concerning systemic risk assessment and mitigation.

Among the other measures that could be adopted are greater attention to content moderation, the promotion and adoption of specific codes of conduct, pursuant to Article 95 of the recent AI Act, and the inclusion of specific warnings for sensitive topics (e.g.: bulletins similar to TV news, mandatory warnings similar to cookie notifications).

Moreover, such economic operators should promote and support investment in the research and development of ethically oriented digital technologies and artificial intelligence systems, structurally involving experts in child development and applied ethics. This interdisciplinary collaboration is essential to ensure that the design of digital products takes into account the developmental, cognitive, and emotional needs of minors, particularly in highly sensitive contexts such as origin searches by adopted individuals.

In parallel, it is essential to implement digital safety measures specifically calibrated to the characteristics of different digital platforms, such as social media and search engines. These measures should be able to proactively prevent the activation of undesired algorithmic connections, which could expose the minor to unsolicited contact with biological family members or to potentially destabilizing content. Such an approach aims not only to protect privacy and safety but also to safeguard the emotional and psychological well-being of adopted minors during delicate journeys of online identity reconstruction.

It is recommended to provide targeted educational materials and guidelines that specifically address the digital risks to which adopted minors may be exposed, such as unexpected online contact with biological relatives or the emotional impact resulting from content recommended by AI-based systems. It is also appropriate to provide professionals with practical tools and adequate training to support adoptive families in understanding and managing the emotional and identity implications connected to the search for origins online. This approach is consistent with the principle of the best interests of the child enshrined in Article 3 UNCRC.

Lastly, it is essential to promote the development of guidelines aimed at supporting adopted minors in developing emotional resilience and building conscious and responsible digital practices.

As far as the category of professionals is concerned, including educators and psychologists, the goal is to provide tools that prevent the scenario in which the minor autonomously initiates an origin search on the web, in the absence of appropriate accompaniment.

Also in this case, it is useful to act already from the stage of professional training, introducing awareness programs on the issue of origin search addressed to adoptive families (both to parents and minors). This helps to increase awareness of the online risks, in line with the preventive and educational function assigned to parental and professional figures under Articles 5 and 18 UNCRC, as well as with the duty of parental responsibility recognised under Articles 2 and 30 of the Italian Constitution. These programs should provide explicit examples of concrete scenarios of exploitation of user vulnerabilities, also based on age and individual needs., echoing the requirements of age-appropriate design and protection of minors' data under Recital 38 and Article 8 GDPR, as well as the Age-Appropriate Design Code which, although originating from the UK, has been influential at the European level.

Certainly, this digital literacy activity requires active listening from parents, so that they learn to interpret their parental duties – such as education, care, protection - in a “digital perspective”: thus, allowing for the introduction of possible alerts as preset functions on devices available to minors, in order to monitor search and access to specific social networks/groups related to the domestic search for origins through parental control tools.

Last only in expository order, but central in relevance, is the category of minors, subjects around whom the entire discipline of adoption revolves and who, in recent times, have attracted the attention of the legislator as particularly active users of the digital environment.

As seen, the increasing use of digital tools has deeply transformed the delicate theme of origin search, which has taken on new forms and characteristics, requiring appropriate tools for accompaniment and protection.

In this context, it is fundamental to provide minors with clear, legally grounded and psychologically respectful guidance, so that the search for origins takes place in a safe and conscious way.

First of all, it is appropriate to encourage the minor not to undertake this journey alone, but to talk to a trusted adult figure, such as a parent, guardian or teacher, who can offer listening, guidance and support.

Secondly, it is essential to promote awareness regarding personal information shared online. Data such as adoptive status, date or place of birth, if publicly disclosed, can make the minor traceable in unexpected and potentially dangerous ways. Therefore, the publication of generic messages (e.g. "*I am looking for my biological family*") on open forums or publicly accessible social platforms should be discouraged. Alternatively, safer digital environments can be considered, such as closed and moderated groups, which offer greater guarantees of confidentiality and protection. It should also be emphasized that caution is needed towards those who might make contact online claiming a family bond. In such situations, it is advisable to take time, avoid immediately providing sensitive information (such as phone numbers, addresses or other personal data), and maintain a vigilant attitude.

Another relevant aspect concerns emotion management. The journey of origin search can indeed stir up complex and conflicting feelings that need to be acknowledged and, where possible, accompanied by competent figures. In this sense, the involvement of a professional may prove particularly useful. It is also fundamental to promote respect for one's own personal story and that of others. Every adopted person has the right to decide whether and how to share their own story, just as biological relatives retain a right to privacy.

Finally, minors should be made aware of their rights regarding access to information about their origins. As seen above, in Italy the legal system recognizes to adopted

persons, once certain requirements are met, the possibility to undertake an official path of reconstructing their family history. Before turning to informal tools such as the internet, it is therefore important to check the existence of appropriate legal channels, being able to count on the support of specialized operators, such as social workers, authorized bodies, or lawyers expert in family law.

If these recommendations were actually followed by all the subjects involved in this delicate scenario, the digital search for origins would be more oriented towards ensuring the delicate balance between identity protection, digital safety, and the right to knowledge, protecting all the figures involved in the field.

Overall, the good practices and recommendations examined and proposed thus far may contribute to making the search for origins not only more structured, but also less exposed to risks concerning the safety of minors. The adoption of an integrated, multi-level, and comparative approach makes it possible to lay the foundation for a complex yet essential intervention: the promotion of digital literacy. This effort goes beyond merely fostering greater awareness among the parties involved. It also aims to achieve genuine empowerment of minors by strengthening their ability to navigate the digital environment in an informed and autonomous manner.

## **7. Digital Education as a Response to (not only digital) Vulnerability: educational practices and regulatory frameworks**

As emphasized in the previous sections<sup>95</sup>, digital literacy represents a cornerstone of minor-centered strategies aimed at transforming vulnerability into agency within digital ecosystems. Moving beyond purely legal and technical interventions, the educational dimension emerges as a key lever for promoting resilience, critical awareness, and informed participation. In the era of pervasive digitalization, digital literacy, defined as the ability to access, understand, evaluate, and create content through technology, is crucial for citizen education and full citizenship, especially among minors<sup>96</sup>. Children and adolescents grow up in a context where the distinction

---

<sup>95</sup> Relevant to this point, see paragraphs 4 and 7 above.

<sup>96</sup> See G. Spadafora, *Processi didattici per una nuova scuola democratica* (vol. 1), Anicita, 2018.

between online and offline is increasingly blurred, with profound effects on social interaction, learning, identity construction, and the exercise of rights.

The following sections expand on this viewpoint by going into greater detail about the theoretical underpinnings and civic significance of digital literacy, particularly in light of the larger framework of democratic citizenship and global social inclusion. The discussion that follows in the next paragraphs places digital and media education at the nexus of civic engagement, ethical responsibility, and human rights, emphasising its crucial role in educating the next generation to navigate, influence, and engage in the digital society.

Digital literacy is the new citizenship<sup>97</sup>, as it allows individuals to participate consciously and critically in public life, countering phenomena such as misinformation, hate speech, and digital exclusion. Digital education is therefore no longer simply a technical matter, but a profoundly civic and social process<sup>98</sup>.

Digital skills are not exclusively technical but include critical, ethical, and relational dimensions that enable citizens - including minors - to actively participate in democratic life, exercise their rights, and recognize their duties, even in the digital space<sup>99</sup>. For this reason, digital literacy is an essential component of global citizenship, inextricably linked to the ability to participate consciously, critically, and responsibly in democratic life. It represents an essential tool for building more inclusive, peaceful, and sustainable societies, as also recognized by the United Nations 2030 Agenda<sup>100</sup>.

The analytical approach adopted in the following sections is grounded in the conviction that digital citizenship education plays a pivotal role in ensuring the meaningful participation and protection of minors within digital environments. Building on the foundations established by the EU regulatory framework, the next section conducts a comparative examination of three countries that have integrated digital civic education into their educational curricula: Italy, the United Kingdom, and

---

<sup>97</sup> See P. Mihailidis, *Civic media literacies: Re-imagining engagement for civic intentionality*, in *Learning, Media and Technology*, 43(2), 2018, pp. 142-164.

<sup>98</sup> See D. Buckingham, *Media education goes digital: an introduction*, in *Learning, Media and technology*, 32(2), 111-119, 2007, pp. 111-119.

<sup>99</sup> See UNESCO, *Digital literacy in education. Policy brief*, 2011. Retrieved from: <https://iite.unesco.org/publications/3214688/>

<sup>100</sup> See United Nations, *Transforming our world: The 2030 Agenda for Sustainable Development*. United Nations General Assembly, 2015. Available at <https://sdgs.un.org/2030agenda>.

France. The goal is not only to evaluate the normative and pedagogical strategies used, but also to determine how these educational systems respond concretely to children's evolving vulnerabilities in increasingly digitalised societies in order to promote a comprehensive, cross-sectoral framework of digital citizenship education that actively involves professionals across education, social services, health, justice, and the digital sector, as well as families and communities, recognising their central role in upholding and advancing children's rights in digital environments<sup>101</sup>.

From this perspective, the OECD highlights that the development of advanced digital skills is essential for training active citizens, capable of navigating the complexity of the 21st century and contributing to the ethical, cultural, and social evolution of the communities in which they live<sup>102</sup>.

This close connection between digital literacy and civic citizenship means that digital education also includes education about legality, democratic participation, civil coexistence, and respect for fundamental rights, including those related to privacy, freedom of expression, and the protection of personal data.

In the context of contemporary digital society, it is essential that digital citizenship promotes an ethic of responsibility, legality, and active participation in an interconnected society. As a result, digital literacy entails teaching people critical thinking skills, online legality, respect for others, and an understanding of their digital rights and responsibilities.

In this perspective, the values and responsibilities associated with digital citizenship must be understood within the broader context of a hybrid reality, where the boundaries between online and offline life are increasingly blurred. This shift calls for a more integrated approach to digital education—one that acknowledges the "onlife"<sup>103</sup> dimension of contemporary experience and its impact on identity, relationships, and the exercise of rights<sup>104</sup>.

---

<sup>101</sup> CURA Blueprint Guidelines, *cit.*

<sup>102</sup> See OECD, *21st-Century Readers: Developing Literacy Skills in a Digital World*, PISA, OECD Publishing, Paris, 2021. Available at <https://doi.org/10.1787/a83d84cb-en>.

<sup>103</sup> L. Floridi, *The onlife manifesto: Being human in a hyperconnected era*, *cit.*

<sup>104</sup> S. Livingstone, E. Helsper, *Gradations in digital inclusion: Children, young people and the digital divide*, in *New media & society*, 9(4), 2007, pp. 671-696.

The analysis presented in the preceding sections highlights the complex and multifaceted risks that threaten personal freedoms, particularly those of minors, if robust safeguards for digital integrity and rights are not fully implemented. In today's interconnected world, the actions of children and adolescents in both physical and digital spaces leave behind data traces that, once aggregated and analysed, generate a level of informational power far exceeding that of the original inputs. This raises serious concerns about profiling, surveillance, and the erosion of privacy.

Minors are especially vulnerable to a wide spectrum of online risks, including cyberbullying, grooming, the non-consensual sharing of images, and exposure to disinformation<sup>105</sup>. At the same time, they are increasingly affected by issues such as digital dependency, social comparison pressure, and premature contact with harmful content. Addressing these challenges requires more than just protective measures; it calls for an educational approach that fosters both safety and the gradual development of digital autonomy.

Digital and citizenship competences are two of the eight key competencies promoted by the Council of European Union<sup>106</sup> from a lifelong learning perspective, from early childhood to adulthood, through formal, non-formal, and informal learning in all contexts, including family, school, workplace, neighbourhood, and other communities.

According to the definitions in the Council of European Union Recommendation of May 22, 2018, digital competence focusses on the technical and cognitive skills required to use digital tools effectively: it entails knowing how to find, evaluate, and communicate information online, as well as how to use various platforms and manage digital risks<sup>107</sup>. Citizenship competence is defined as the ability to act responsibly and actively participate in civic and social life while understanding social, economic, legal,

---

<sup>105</sup> D. Smahel, H. Machackova, G. Mascheroni, L. Dedkova, E. Staksrud, K. Ólafsson, U. Hasebrink, *EU Kids Online 2020: Survey results from 19 countries*, 2020.

<sup>106</sup> Council of the European Union. (2018). Council Recommendation of 22 May 2018 on key competences for lifelong learning (2018/C 189/01). [https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32018H0604\(01\)](https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32018H0604(01)).

<sup>107</sup> Council of the European Union (2018/C 189/01), *cit.* See in Annex, point 4: “*Digital competence involves the confident, critical and responsible use of, and engagement with, digital technologies for learning, at work, and for participation in society. It includes information and data literacy, communication and collaboration, media literacy, digital content creation (including programming), safety (including digital well-being and competences related to cybersecurity), intellectual property related questions, problem solving and critical thinking*”.

and political structures and concepts, as well as their global evolution and sustainability principles<sup>108</sup>.

The concept of digital literacy has gradually expanded to include an educational component, resulting in the concept of digital citizenship education. This shift reflects the need to promote structured learning that develops broader and deeper skills, rather than simply mastering the technical aspects of digital tools.

The digital citizenship education paradigm is systematically adopted in the Digital Citizenship Education Handbook<sup>109</sup> and serves as a key European reference for the definition, promotion, and implementation of digital citizenship education. The text provides a clear and comprehensive conceptual framework for linking responsible use of digital technologies to democratic principles, human rights, and the rule of law. The handbook, organised around ten competency domains, offers practical and pedagogical tools for teachers, educators, and education policymakers with the goal of developing active, informed, and inclusive digital citizens. Its function is both normative and transformative: it promotes civic education that is current with the challenges of the digital world, focussing on participation, ethics, and social cohesion.

In line with this vision, the European Commission further clarifies the idea of digital literacy and its close connection to citizenship competence.

With the Digital Competence Framework for Citizens (DigComp), European Commission defines digital citizenship as the set of skills needed to use digital technologies safely, ethically, and participatively in education, work, information, and civic engagement<sup>110</sup>.

---

<sup>108</sup> Council of the European Union (2018/C 189/01), *cit.* See in Annex, point 6: “*Citizenship competence is the ability to act as responsible citizens and to fully participate in civic and social life, based on understanding of social, economic, legal and political concepts and structures, as well as global developments and sustainability*”.

<sup>109</sup> J. Richardson, E. Milovidov, *Digital citizenship education handbook: Being online, well-being online, and rights online*, Council of Europe, 2019.

<sup>110</sup> R. Vuorikari, S. Kluzer, Y. Punie, *DigComp 2.2: The Digital Competence Framework for Citizens-With new examples of knowledge, skills and attitudes*, 2022. DigComp's framework, developed as a scientific project by the Joint Research Centre (JRC) with significant input from various stakeholders, was published in 2013 and has since become an essential reference point for the formulation and implementation of digital skills strategies at both the European and Member State levels. The first edition, titled DigComp: A Framework for Developing and Understanding Digital Competence in Europe, describes digital competence by starting with the needs that every citizen of the information and communication society has. The DigComp model is based on these needs, which include being informed, interacting, expressing oneself, protecting oneself, and dealing with

Although the younger generations are considered digital natives<sup>111</sup>, it is important to remember that digital technology is not always designed to meet these new demands. As we have seen in previous sections, minors are more vulnerable to the dangers of the internet. As a result, adult figures, particularly teachers, must be aware of the influence they can have on children's development and their relationship with information and communication technology. Educators must therefore develop effective digital skills.

In 2017, the European Commission developed a framework for teachers and educators' digital skills. The "European Framework for the Digital Competence of Educators: DigCompEdu"<sup>112</sup> is divided into six competency areas: professional engagement; digital resources; teaching and learning; assessment; empowering learners; facilitating learners' digital competence.

DigCompEdu is a model that allows for the description of digital pedagogical competence, the level of mastery, and self-assessment<sup>113</sup>.

The European Commission has consistently underscored the strategic importance of digital competence as a key enabler of economic growth, innovation, and social cohesion. In addition to the DigComp framework, several major policy initiatives reflect this commitment - most notably the Digital Education Action Plan 2021 -

---

technological and digital environment problems. The DigComp model matrix consists of five dimensions. Dimension 1 contains the title of the competence area. Dimension 2 indicates the competence's title and description. Dimension three is dedicated to mastery levels. Dimension 4 provides examples of knowledge, skills, and attitudes that are not differentiated into mastery levels. Dimension 5 demonstrates the competence's applicability in employment and learning scenarios. A three-phase update procedure was started, utilising the DigComp first edition matrix. The first update was R. Vuorikari, Y. Punie, S. C. Gomez, G. Van Den Brande, *DigComp 2.0: The digital competence framework for citizens*, 2016. The second update was G. S. Carretero, R. Vuorikari, Y. Punie, *DigComp 2.1: The Digital Competence Framework for Citizens with eight proficiency levels and examples of use*, 2017. Finally, *DigComp 2.2: The Digital Competence Framework for Citizens - With new examples of knowledge, skills, and attitudes, cit.*

<sup>111</sup> M. Prensky, *H. sapiens digital: From digital immigrants and digital natives to digital wisdom*, in *Innovate: journal of online education*, 5(3), 2009.

<sup>112</sup> C. Redecker, *European Framework for the Digital Competence of Educators: DigCompEdu*, Y. Punie, (ed.), EUR 28775 EN. Publications Office of the European Union, Luxembourg, 2017.

<sup>113</sup> "Selfie for teachers" is a tool based on DigCompEdu managed by the European Commission that allows teachers to evaluate their digital competence. It is one of the initiatives of the action plan or the commission for digital education. Available in <https://education.ec.europa.eu/selfie-for-teachers>.

2027<sup>114</sup>, which outlines a vision for high-quality, inclusive, and accessible digital education across the EU, and the Digital Decade Policy Programme 2030<sup>115</sup>, which sets concrete targets for digital skills, infrastructure, and public services within the broader context of Europe's digital sovereignty and resilience.

Through these initiatives, the European Union is actively fostering the development of both basic digital literacy, essential for everyday life and civic participation, and advanced digital skills, such as data literacy, coding, and artificial intelligence, which are increasingly crucial for employability and competitiveness. This dual focus aims not only to support the digital transformation of education and the labour market, but also to promote digital inclusion, ensuring that all citizens, regardless of age, background, or socioeconomic status, can engage meaningfully and safely in the digital society. Particular attention is given to children and adolescents, who are among the most vulnerable users of digital technologies and therefore require targeted educational support and protection to develop the critical, ethical, and technical skills needed to navigate digital environments responsibly.

As digital technologies evolve rapidly, the concept of digital competence must also expand to address the emerging challenges posed by artificial intelligent (AI) systems. Beyond ensuring broad access and inclusion, especially for vulnerable groups such as minors, it is increasingly necessary to equip all citizens with the ability to critically engage with the technologies shaping their environment. In this broader educational vision, digital literacy becomes the stepping stone toward more advanced and nuanced forms of competence, most notably, AI literacy, which demands not only technical understanding but also ethical sensitivity, critical thinking, and social responsibility in the face of algorithmic decision-making and data-driven processes.

In this context, the European Union has launched initiatives to enhance awareness of AI and data in education, starting with the Ethical Guidelines for Educators on Using

---

<sup>114</sup> European Commission: Directorate-General for Education, Youth, Sport and Culture, *Digital education action plan 2021-2027 – Improving the provision of digital skills in education and training*, Publications Office of the European Union, 2023, <https://data.europa.eu/doi/10.2766/149764>.

<sup>115</sup> <https://digital-strategy.ec.europa.eu/en/library/digital-decade-policy-programme-2030>.

AI and Data in Teaching and Learning<sup>116</sup>, aiming to increase awareness of AI and data in education.

## **8. The role of educational institutions and educational alliances: a comparison between Italy, United Kingdom, and France**

Educational institutions play an important role in promoting digital citizenship. They are expected to educate not only on the use of technology, but also on its critical, informed, and responsible application. In this context, establishing educational alliances between schools, families, and communities becomes critical.

From this perspective, educational policies serve as a starting point for providing schools with the tools and vision required to address the challenges of digital transformation, all while strengthening the educational relationship as the foundation of learning.

Regulatory strategies governing digital literacy and citizenship education vary across European contexts, reflecting distinct cultural visions and educational priorities.

In Italy, the National Digital School Plan<sup>117</sup> (hereinafter PNSD) identify innovation strategies for Italian schools in the digital age, with a focus on the epistemological and cultural dimensions of the educational relationship<sup>118</sup>.

---

<sup>116</sup> See European Commission: Directorate-General for Education, Youth, Sport and Culture, Ethical guidelines on the use of artificial intelligence (AI) and data in teaching and learning for educators, Publications Office of the European Union, 2022, <https://op.europa.eu/en/publication-detail/-/publication/d81a0d54-5348-11ed-92ed-01aa75ed71a1/language-en>.

<sup>117</sup> Piano Nazionale Scuola Digitale, DM 851 del 27 ottobre 2015, [https://www.istruzione.it/scuola\\_digitale/index.shtml](https://www.istruzione.it/scuola_digitale/index.shtml).

<sup>118</sup> In light of the profound digital transformation that is affecting the Italian school system, the PNSD emphasises the importance of consciously and responsibly integrating technology into educational processes. Despite the emphasis on innovation, the Plan emphasises the importance of keeping the relationship between teacher and student at the heart of the educational process, recognising that human interaction is still an irreplaceable component even in the age of digital education (Since "technology cannot elide this fundamental human relationship and no educational step can be separated from an intensive teacher-student interaction" (PNSD, 2015, p. 7).

As part of this plan, specific figures such as digital animators<sup>119</sup> and innovation teams were introduced to foster informed use of digital technologies in educational settings.

Following that, the Italian Minister of Education approved issued Decree No. 161 on June 14, 2022, approving the School Plan 4.0<sup>120</sup>, which was funded by the Italian Recovery and Resilience Plan. This builds on the experience of the previous PNSD, which aimed to transform country's classrooms into ecosystems for integrated digital teaching in which analogue and digital, physical and digital, school and local communities converged to form an innovative and well-organised project. Although these efforts mark a structural shift, explicitly aligned with European frameworks such as DigComp 2.2<sup>121</sup> and DigCompEdu<sup>122</sup>, the current approach remains predominantly focused on infrastructure and the general enhancement of basic digital skills. It lacks, however, sufficient regulatory and organizational measures to ensure the systematic protection of minors in digital environments, as well as meaningful progress in digital literacy.

The Italian Law No. 92 of August 20, 2019<sup>123</sup>, which introduced civic education into the national school curriculum, represents a shift towards a more forward-looking and systemic vision, as does the growing recognition of the importance of prioritising digital and AI education to equip future generations with the skills required in a rapidly evolving digital society.

---

<sup>119</sup> The PNSD's Action #28 section provides a comprehensive and official description of the Digital Animator profile, outlining their responsibilities, areas of intervention, and strategic significance in the process of digitally transforming Italian schools. The Digital Animator must create projects in three crucial areas in order to fulfil Action #28: - internal school training, which is accomplished by planning and directing training sessions and events that involve the school community; - participation of the school community, promoting students', families', and local stakeholders' involvement in order to establish a common digital culture; - the development of novel, sustainable, and technologically and methodologically sound solutions that meet the needs of the school. This position is not just a technical support role; it is a systemic role. It receives training through specialised programmes that support educational innovation and digitisation, in line with the initiatives delineated in the Three-Year Educational Offer Plan (PTOF).

<sup>120</sup> Decree of the Italian Minister of Education, 14 June 2022, n. 161, which adopts "Piano scuola 4.0", provided for by *Piano nazionale di ripresa e resilienza*, <https://www.mim.gov.it/-/decreto-ministeriale-n-161-del-14-giugno-2022>.

<sup>121</sup> *DigComp 2.2: The Digital Competence Framework for Citizens-With new examples of knowledge, skills and attitudes, cit.*

<sup>122</sup> *European Framework for the Digital Competence of Educators: DigCompEdu, cit.*

<sup>123</sup> Law 20 August 2019, n. 92 "Introduzione dell'insegnamento scolastico dell'educazione civica (Introduction of civic education teaching in schools)", <https://www.gazzettaufficiale.it/eli/id/2019/08/21/19G00105/sg>.

The law promotes the development of responsible and active citizenship by encouraging full and informed participation in civic, cultural, and social life, in accordance with the principles of rights, duties, and rule of law and duties.

In particular, Law 92/2019 establishes “digital citizenship” as one of the three pillars on which to build the 33 transversal hours of the new teaching, along with the “constitution” and “sustainable development”<sup>124</sup>. From this perspective, the emphasis is not on technological literacy, but on a more proactive approach centred on the five areas that comprise it: the Internet and ongoing change, media education, information education, quantification and computation: data and artificial intelligence, digital culture and creativity<sup>125</sup>.

Law 92/2019, which established civic education as a transversal subject, identifies in Article 3 a set of skills and learning objectives related to three major thematic areas: the “constitution” (in the broad sense, national and international law, legality, and solidarity); “sustainable Development” (and environmental education, as well as knowledge and protection of heritage and territory); and “digital citizenship”<sup>126</sup>. This emphasises the significance of digital citizenship education as a central theme with broad educational goals. These objectives address both cognitive and non-cognitive skills, including the digital dimension, and use their transversality to make meaningful connections between learning areas.

---

<sup>124</sup> Decree of the Italian Minister of Education, n. 183, 7 September 2024, “*Adozione delle Linee Guida per l'insegnamento dell'educazione civica*”, Gazzetta Ufficiale della Repubblica Italiana, 2024, [https://www.istruzione.it/educazione\\_civica/norme.html](https://www.istruzione.it/educazione_civica/norme.html).

<sup>125</sup> S. Past, a P.C. Rivoltella, *Crescere onlife. L'Educazione civica digitale progettata da 74 insegnanti-autori*. Morcelliana Scholé, 2022.

<sup>126</sup> Article 5 of Law n. 92/2019, which details the essential digital skills and knowledge to be developed in relation to the core theme of digital citizenship, identifies seven areas of interest that are directly linked to the areas of the European Framework of DigComp 2.2.

1. Analyse, compare, and critically assess the credibility and dependability of sources.
2. Interact with various digital technologies and determine the best method of communication for a given situation.
3. Obtain information and participate in public debate using public and private digital services.
4. Understand the rules of conduct when using technology.
5. Create and manage a digital identity, protect one's reputation, and manage and secure data.
6. Learn about digital services' privacy policies.
7. Be able to identify and avoid health risks and threats to one's physical and psychological well-being, as well as understand how technologies affect them.

In 2023, the United Kingdom passed the *Online Safety Act*<sup>127</sup>, one of Europe's most advanced pieces of legislation for protecting minors online, imposing a duty of care on platforms.

Section 166 of the *Online Safety Act* adds a new section 11A to the Communications Act, requiring the Office of Communications (Ofcom)<sup>128</sup> to develop and publish a media literacy strategy within one year of the *Online Safety Act*'s passage.

Ofcom's mandate includes the development of a media literacy programme called "Making Sense of Media"<sup>129</sup> (hereinafter MSOM). The MSOM focusses on two key dimensions: people and online platforms. The documented work focusses on platform interventions to promote media literacy, analysing how regulated services address this issue directly "on-platform" and developing a set of best practice principles for social media, search engines, video sharing, and gaming services.

MSOM's goal is to identify what works and what doesn't work online in order to help users improve their media skills.

Ofcom has developed 14 principles for "good media literacy by design" as part of the MSOM programme, specifically for social media, search, video sharing, and gaming services. Adopting these principles would allow platforms to foster safer and more rewarding use of their services, resulting in a positive, sustainable, and beneficial experience for both users and online service providers.

Keeping Children Safe in Education<sup>130</sup> (hereinafter KCSIE), a mandatory regulatory guide for all schools and colleges in England published by the Department for Education, is particularly noteworthy. It establishes the legal obligations that schools must meet to protect and promote the well-being and safety of minors under the age of 18 in their facilities.

The document outlines how school staff and leaders should identify and manage the risks of abuse, neglect, bullying, exploitation, and other forms of harm. Furthermore, in the "Online Safety" section (paragraphs 135 and 136), the guide emphasises the

---

<sup>127</sup> Uk Parliament, *Online Safety Act*, 2023, *cit.*

<sup>128</sup> Ofcom's role under *Online Safety Act*, <https://www.legislation.gov.uk/ukpga/2023/50>, *cit.*

<sup>129</sup> Available at <https://www.ofcom.org.uk/media-use-and-attitudes/media-literacy/making-sense-of-media>.

<sup>130</sup> UK Department for Education, *Keeping children safe in education: Statutory guidance for schools and colleges*, 2024, <https://www.gov.uk/government/publications/keeping-children-safe-in-education--2>.

critical importance of an effective and integrated institutional approach to protect, educate, and intervene in the event of risks associated with the use of technology by pupils, students, and school personnel.

After identifying four major areas of online risk<sup>131</sup>, the guide states that school governance bodies must integrate online safety as a cross-cutting theme into safeguarding policies and curriculum, including teacher training, parent involvement, and a clear definition of child protection coordination roles<sup>132</sup>.

School governance bodies are in charge of incorporating online safety as a cross-cutting theme into safeguarding policies and curricula, which includes teacher training, parent involvement, and clearly defined child protection coordinator roles<sup>133</sup>.

---

<sup>131</sup> According to paragraph 135 of the KCSIE: “*The breadth of issues classified within online safety is considerable and ever evolving, but can be categorised into four areas of risk: content: being exposed to illegal, inappropriate, or harmful content, for example: pornography, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, extremism, misinformation, disinformation (including fake news) and conspiracy theories. contact: being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes. conduct: online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying, and commerce: risks such as online gambling, inappropriate advertising, phishing and or financial scams*”.

<sup>132</sup> The KCSIE’s paragraph 140 states that it is the duty of schools to guarantee suitable filtering and monitoring systems, modifying them in accordance with particular risks and the influence on the curriculum.

<sup>133</sup> In this context, according to KCSIE paragraphs 102 and 103, the Designated Safeguarding Lead (hereinafter DSL) is an important component of school governance for child protection. This position, mandated by current safeguarding legislation, is assigned to a member of the senior leadership team and carries significant strategic and operational responsibilities. The DSL is responsible for ensuring that the institution responds to risks or vulnerabilities involving students in a timely, appropriate, and regulatory-compliant manner.

The KCSIE’s Annex C describes the broad areas of responsibility and activities associated with the role DSL. Organisationally, he has the authority and resources to manage protection processes on his own, including coordinating reports and referring them to appropriate authorities. From this standpoint, the DSL serves as a point of reference for multi-agency collaboration, such as interprofessional strategies and interdisciplinary prevention and intervention conversations. In terms of education and training, the DSL is responsible for keeping school staff up to date on child protection issues, including digital environment risks, and incorporating this information into curricular and professional development plans. He is also responsible for keeping child protection files secure, confidential, and traceable, as well as ensuring proper transmission during school transitions. A key aspect of the role is to foster a protective school culture by disseminating and implementing safeguarding and child protection policies. The DSL also plays a preventative and inclusive role, helping to identify vulnerable students’ educational and psychosocial needs early on, promoting their well-being, and promoting educational equity.

In early 2023, the French Ministry of National Education published the document *Numérique pour l'éducation 2023-2027: la vision stratégique d'une politique publique partagée*<sup>134</sup> which defined a national strategy for digital education for the five-year period 2023-2027.

The document aims to create a shared ecosystem that supports all levels of education, based on four strategic axes.

In terms of educational governance, the document describes a series of actions aimed at improving educational cooperation in digital technology at the national and local levels, including the development of tools for monitoring progress (shared dashboard, indicators). The strategy also calls for investments in *Territoires numériques éducatifs*, with projects such as providing individual devices to college and high school students beginning in 2024. This aims to narrow the digital divide between regions and provide equal opportunities for digital learning.

The document describes the development of a digital skills and citizenship curriculum throughout the school year to develop digital skills (critical thinking, coding, and AI literacy), with the goals of professional and social growth, as well as systematic awareness-raising about responsible social media use and cyberbullying prevention.

The third strategic axis emphasises the importance of fostering an educational community of shared and accessible tools, known as *communs numériques* and *compte ressources*, to facilitate access to educational resources and the development of an inclusive and sustainable digital offering for all school communities.

Finally, the document outlines the plan to renew the ministerial information system based on the principles of efficiency, interoperability, user experience, and environmental sustainability (eco-responsibility), with the goal of simplifying services for staff and families.

The document is important at the institutional level because it outlines a shared public policy aimed at a broad range of stakeholders (states, regions, institutions, EdTech, and associations) and lays the groundwork for participatory governance of digital

---

<sup>134</sup> Ministère de l'Éducation nationale, *Numérique pour l'éducation 2023-2027 : La vision stratégique d'une politique publique partagée*, 2023, <https://www.education.gouv.fr/feuilles-de-route-450426#:~:text=La%20strat%C3%A9gie%20num%C3%A9rique%20pour%20la,transformation%20du%20syst%C3%A8me%20d'information>.

education in schools. It is also accompanied by *feuille de route*; thematic roadmaps such as one for data and algorithms in 2024-2027, which supplement the strategic vision with specific operational measures.

Beyond the institutional context, France promotes digital and AI literacy through various policy initiatives that are part of a comprehensive national strategy. The *Éducation au numérique* programme<sup>135</sup>, promoted by the *Commission Nationale de l'Informatique et des Libertés National* (hereinafter CNIL). This comprehensive set of educational resources is designed for teachers, students, and families, with the goal of raising awareness among young people about the responsible use of personal data and promoting knowledge of digital rights in accordance with the GDPR. The proposed activities, which include thematic worksheets, workshops, educational games, and training modules, are in line with the competencies established by the *Cadre de Référence des Compétences Numériques*<sup>136</sup> and are fully compatible with the teaching of EMI. The CNIL's initiative contributes to the development of critical and responsible digital citizenship, focussing on the concepts of online reputation, privacy, digital identity, and security. This multidimensional approach is an integrated model of digital civic education that strengthens the link between technological literacy and legal and ethical awareness in French schools.

A comparison of the United Kingdom and France reveals significant similarities, particularly an integrated approach to digital literacy that combines awareness of digital rights, personal data protection, and a comprehensive view of citizenship. This approach, which is firmly rooted in European legislation and the major digital competence frameworks, acknowledges schools as critical players in the formation of informed and responsible digital citizens.

---

<sup>135</sup> Available at <https://www.cnil.fr/fr/mots-cles/education-numerique>.

<sup>136</sup> Décret n. 2019-919 du 30 août 2019 relatif au développement des compétences numériques dans l'enseignement scolaire, dans l'enseignement supérieur et par la formation continue, et au cadre de référence des compétences numériques, <https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000039005162>. The *Cadre de Référence des Compétences Numériques* is an official framework adopted in France that has been in effect since 2019, defining essential digital skills for students from primary school to university, as well as adults in vocational training. The CRCN, which is based on DigComp framework, organises 16 digital skills into five thematic areas (information and data; communication and collaboration; content creation; protection and security; digital environment), each with eight levels of proficiency. These skills are certified using the Pix platform, with certifications given at the end of cycle 4 (*collège*) and the final cycle of high school (*lycée*).

Although Italy, the United Kingdom, and France all include digital citizenship within their educational agendas, notable differences persist in the ways these countries structure their school systems and design governance models for digital education. These divergences influence how policies are implemented, the degree of institutional coordination involved, and the extent to which schools are empowered to act as agents of digital transformation.

In Italy, despite the release of a Digital Civic Education Curriculum in 2018<sup>137</sup>, digital education is integrated into the transversal teaching of civic education, which remains strongly linked to the legal-pedagogical importance of teaching the constitution and its principles. Furthermore, civic education instruction in Italian schools remains uneven: there is a lack of structured and common tools for monitoring and evaluating the courses offered, as well as a coordinated and systematic strategy for teacher training<sup>138</sup>.

---

<sup>137</sup> MIUR-Ministero dell'Istruzione, dell'Università e della Ricerca, Curriculum di Educazione Civica Digitale, Roma, 2018, <https://scuoladigitale.istruzione.it/iniziative-competenz/sillabo-suleducazione-civica-digitale/>. The Curriculum suggests creating "positive strategies" that will allow students to "appropriate digital media, moving from passive consumers to critical consumers and responsible producers of content and new architectures" (MIUR, 2018, p. 5). The 2018 syllabus emphasises critical thinking and responsibility education, which are defined as awareness of the consequences of one's actions in the digital world, in promoting skill development.

<sup>138</sup> The law introducing civic education into the Italian education system requires the implementation of an integrated approach to this curricular area. At the same time, the law and the Guidelines for Implementation are ambiguous. On the one hand, this document seems to support the transversal nature of civic education. This approach is supported by statements in the Guidelines (Cf. note n. 106; [https://www.istruzione.it/educazione\\_civica/norme.html](https://www.istruzione.it/educazione_civica/norme.html)) that describe its relationship to other subjects in the curriculum, as well as an encouragement to avoid the simple juxtaposition of content from different subjects.

According to the teaching organisation, the number of hours dedicated to teaching civic education will be jointly assigned to multiple teachers from the same class council, one of whom will serve as coordinator. On the other hand, in other passages, this choice appears to be partially questioned, such as when it is explicitly stated that teaching activities can be carried out "by one or more teachers" and, in secondary schools, when it is decided to assign teaching to the teacher of "legal subjects" (if such subjects are included in the curriculum), albeit in collaboration with other members of the class council. Article 11 of the law explicitly mentions the "prospect of a possible modification to the timetable that would add an hour of civic education," implying that the transversal approach could be replaced by the introduction of a "separate" subject. Furthermore, the established number of hours is "derived" from the timetable of the subjects and areas already included in the curriculum.

The decision to take a "transversal" approach appears to be more influenced by organisational and contingent needs (such as maintaining staff and timetables and the unavailability of specific resources) than by a clear conceptual and methodological choice. These fundamental ambiguities give rise to a number of issues regarding

In the United Kingdom, digital citizenship education is more operational and regulatory, with a strong emphasis on minors' online safety (duty of care) and the role of digital platforms as co-responsible.

In France, a long-term strategic approach is taken, based on multilevel governance and the development of a shared public policy, with a broad vision that includes training, infrastructure, territorial equity, and sustainability.

The differences that emerged, particularly between the UK's regulatory-operational approach and France's strategic-systemic vision, enabled us to identify complementary elements to Italy's critical issues. On the one hand, the UK experience has demonstrated the value of a clear regulatory framework that defines shared responsibilities among educational institutions, digital platforms, and families<sup>139</sup>. On the other hand, the French approach has demonstrated the importance of multilevel governance, which can organically integrate teacher training, equal access, and digital infrastructure<sup>140</sup>. The comparative perspective has influenced the development of common policy proposals in terms of coherence, monitoring, and systematicity, with

---

planning, teaching methodology selection, and assessment. For example, on the one hand, the possibility of organising and managing the minimum 33 hours of teaching hours in a modular manner, rather than distributing them throughout the school year, is increasing. On the other hand, it is expected that a separate civic education assessment will be formally administered on a regular basis (at the end of each term or four-month period) and at the conclusion of each term. Actually, in the name of autonomy, schools are supposed to address and resolve these problems, but there are no guarantees that they will be able to do so.

<sup>139</sup> In the United Kingdom, for example, the adoption of the *Online Safety Act* 2023 imposes specific protection duties on digital platforms, and the development of a clear media literacy strategy has begun, expanding Ofcom's mandate. According to *Online Safety Act* 2023, Chapter 6 - Codes of Practice and Guidance, Ofcom is now responsible for enforcing the new legislation, as well as developing and overseeing mandatory codes of conduct for online platforms. Ofcom seeks to maintain a balance between freedom of expression and child protection by implementing the Protection of Children Codes (April 2025, <https://www.ofcom.org.uk/online-safety/illegal-and-harmful-content/statement-protecting-children-from-harms-online>) and holding public consultations.

<sup>140</sup> In France, the *Cadre de Référence des Compétences Numériques* oversees the development of digital skills across the board, with a progression of levels and standardised certification. is more than just a technical framework; it is also a pedagogical framework aimed at developing informed, autonomous, and responsible digital citizens. Its significance lies in the strengthening of four critical dimensions: - Inclusion: It helps to bridge the digital divide by providing a gradual path to skill acquisition. - Formative assessment: It enables the transparent and continuous observation and measurement of progress. - Integrated education: It encourages transversal teaching, which links digital skills to all disciplines. - Active citizenship: It teaches young people not only how to use digital tools, but also about their ethical, social, and political implications.

the goal of promoting and disseminating digital civic education as a tool for informed participation by children and all stakeholders in digital society.

## **9. Bridging the digital divide: empowering online safety through digital education**

Digital education is an effective tool for youth empowerment and social inclusion, capable of closing educational gaps and encouraging active and informed citizenship.

Schools and community learning centres play an important role in developing these competencies by using digital technologies as tools for creativity and active learning<sup>141</sup>. They also help foster critical thinking, resilience, and support families in guiding children's use of technology. Expanding school access and investing in teacher training can better connect internet use with educational opportunities, helping address the significant digital skill gaps among younger students<sup>142</sup>. As early as 2014, the UN Committee on the Rights of the Child recommended that member governments incorporate digital literacy into their national school curricula<sup>143</sup>.

In light of this, principles underpinning in all previous considerations could make a significant contribution to addressing the current gaps and areas of disadvantage within the Italian system, particularly in the fields of digital education and online child protection, as highlighted through comparative analysis with approaches taken in Italy, the United Kingdom and France.

Such a proposal would advocate for a more relational approach to digital literacy, raise awareness, and provide adequate psychosocial support for minors who are especially vulnerable in digital contexts<sup>144</sup>.

---

<sup>141</sup> S. Chaudron, R. Di Gioia, M. Gemo, *Young Children (0-8) and Digital Technology: A qualitative study across Europe*, EUR 29070 EN, Publications Office of the European Union, Luxembourg, 2017.

<sup>142</sup> J. Byrne, D. Kardefelt-Winther, S. Livingstone, M. Stoilova, *Global Kids Online research synthesis, 2015–2016*, Research Report, UNICEF Office of Research–Innocenti and London School of Economics and Political Science, 2016.

<sup>143</sup> Committee on the Rights of the Child Report of the 2014 day of General Discussion on “*Digital Media and Children’s Rights*”, par. N. 109, [https://www.ohchr.org/sites/default/files/Documents/HRBodies/CRC/Discussions/2014/DGD\\_report.pdf](https://www.ohchr.org/sites/default/files/Documents/HRBodies/CRC/Discussions/2014/DGD_report.pdf).

<sup>144</sup> CURA Blueprint Guidelines, cit., pp. 9-11.

Strengthening a relational perspective in digital literacy and awareness promotion appears to be critical for making interventions more effective and meaningful. This approach fosters family engagement and supports the development of critical awareness of digital technologies through structured communication strategies and attention to emotional well-being.

The implementation of educational programmes that teach children, parents, and educators about online risks, ethical considerations, and responsible digital citizenship has the potential to close the educational gap. To be truly effective, such programmes should be integrated into both school curricula and broader societal contexts, and include modules on topics such as the attention economy, content creation, peer pressure, and the ethical implications of online sharing. These programmes, if integrated into school curricula and promoted at the EU level, have the potential to standardise digital education, making it more accessible and mandatory. For example, implementing a standardised certification programme for adolescents that is flexible based on their developmental maturity could ensure that all students acquire essential digital skills, thereby reducing regional and socioeconomic disparities.

This includes not only teaching critical and responsible technology use, but also strengthening educational relationships and promoting parental involvement to foster a shared understanding of the collaborative role families play in developing critical awareness of digital technologies. Supporting families through training opportunities, emotional resources, and structured dialogue, such as workshops and targeted materials, can enhance trust and communication between parents and children, encouraging more effective and authoritative parenting practices in the digital sphere.

Promoting greater parental involvement in their children's digital technology use, as well as encouraging authoritative parenting practices, can help families communicate and trust more effectively. In contexts where engaging the most vulnerable families presents a challenge, initiatives such as interactive workshops and accessible educational resources can foster open dialogue on online safety, digital ethics, and responsible behaviour. Adopting a relational approach can support adolescents in developing a digital safe base, enabling them to navigate the online environment with greater confidence and security<sup>145</sup>.

---

<sup>145</sup> CURA Blueprint Guidelines, cit., p. 11.

Finally, it is critical to implement psychosocial support that addresses the unique needs of minors as

Providing mental health, psychological, and sociological support services to children exposed to online risks represents a fundamental step in mitigating the adverse effects associated with digital technologies. Specialised services aimed at supporting vulnerable users can play a critical role in addressing phenomena such as cyberbullying, online abuse, and exposure to harmful content. To ensure broad and equitable access, these services should be systematically integrated into educational institutions and community settings, thereby reaching all students irrespective of their socioeconomic background<sup>146</sup>.

Consequently, promoting the development of children's rights impact assessments as part of broader fundamental rights monitoring represents a critical step toward ensuring that digital products and services are safe, appropriate, and responsive to the specific needs of minors. Embedding such assessments within product conformity and safety evaluation processes can assist economic operators in aligning with child protection standards, particularly in regulatory environments where dedicated online safety legislation remains under development.

## **10. Conclusions**

In today's digital environment, where children's presence is both pervasive and yet often rendered invisible, the challenge of developing tools capable of recognising and addressing their vulnerabilities has become inescapable. To respond to this challenge, not by offering definitive solutions, but by outlining a coherent, multisectoral, and child-centred operational path resulted a first attempt towards a safer and child-friendly approach to digitalization of services and product.

The ultimate goal is not merely to shield children from digital risks, but to contribute to the construction of an environment that embraces childhood and adolescence in all their complexity, supporting their emotional, relational, cognitive, and identity-related needs. From this perspective, protection is not conceived as a defensive or

---

<sup>146</sup> CURA Blueprint Guidelines, cit., pp. 11-12.

restrictive measure, but rather as an enabling condition for meaningful and informed participation in digital society.

The adopted approach, combining legal frameworks, technical safeguards and educational initiatives, allows us to move beyond the traditional dichotomy between protection and participation. Such integration is essential not only to address the layered nature of children's vulnerabilities, as discussed in the first part, but also to counteract the fragmentation of interventions, institutional inertia, and the tendency to shift responsibility solely onto parents or the children themselves. The underlying logic is that of shared responsibility: between adults and minors, between public and private actors, between central institutions and local communities.

The educational dimension highlights how achieving a truly inclusive form of digital citizenship requires the joint commitment of schools, families, and broader communities, working together to develop coherent, accessible learning pathways that build upon existing resources. In this light, digital education emerges not as a secondary or optional competence, but as a structural prerequisite for exercising rights in the digital realm, for building meaningful relationships, for safeguarding personal integrity, and for developing a critical understanding of digital languages and dynamics.

A particularly emblematic case is that of adopted children searching for their origins: a growing phenomenon that illustrates the potential of the digital sphere as a space of knowledge and self-affirmation, but also its profound risks when not accompanied by emotional support, adequate digital skills, and institutional oversight. In this regard, the blueprint policies aim to fill a normative and practical gap, by proposing a reconsideration of access thresholds and service interactions, and by promoting relational and educational frameworks capable of combining self-determination with protection.

Ultimately, a model of digital childhood governance that is actionable, sustainable and, above all, attuned to the lived realities of children and adolescents will contribute to building a digital ecosystem that is more equitable, inclusive, and respectful of minors' dignity and fundamental rights. At a time when the rapid pace of technological innovation threatens to produce new forms of exclusion and fragility, these guidelines serve as instruments of guidance and collective responsibility. They invite all stakeholders (institutions, professionals, families and platforms) to recognise

the complexity at hand and to transform it into an opportunity for shared growth and care.



## **YES, WE CAN...AND WE MUST! CHANGING THE NARRATIVE OF CHILDREN'S RIGHTS PROTECTION IN THE DIGITAL ENVIRONMENT THROUGH A CHILD-CENTERED APPROACH. THE LESSON FROM THE U.K. CHILDREN'S CODE**

Sara Rigazio\*

### **Abstract**

In the face of empirical data confirming that children and young people spend a great deal of time online, today's reality delivers an equally alarming result: the Internet was not conceived and designed with the idea that users could also be minors. This represents a serious shortcoming that could, however, be remedied where a genuinely child-centered approach is chosen, that is, an approach based on the founding principles of the UN Convention on the Rights of the Child (CRC): the best interests, the evolving capacities and the right to be heard. Together with the essential contribution and role played by family, institutions and stakeholders, the narrative on the protection of children online could take on a different and more appropriate direction, focusing on the fundamental dimension of the *promotion* of children's rights and their agency.

The UK Children's Code represents, in this regard, a concrete model to look at with extreme interest. Its circulation, influence and success – with different nuances – proves, in fact, that one of the key elements in this topic is represented by the *empowerment* – both of the single minor and of the collectivity – in order to maintain and preserve what makes and builds our identity: human dignity.

---

\* Assistant Professor of Comparative Law, Department of Political Sciences and International Relations, University of Palermo. Double blind peer reviewed contribution.

## Table of contents

YES, WE CAN...AND WE MUST! CHANGING THE NARRATIVE OF CHILDREN'S RIGHTS PROTECTION IN THE DIGITAL ENVIRONMENT THROUGH A CHILD-CENTERED APPROACH. THE LESSON FROM THE U.K. CHILDREN'S CODE .....	173
Abstract.....	173
Keywords.....	174
1. Introduction.....	174
2. The U.K. Children's Code in the prism of the CRC and of the design discourse .....	177
3. The impact of the Code: concrete results .....	184
4. Imitation and circulation of the Code: does it work?.....	187
4. A child centered approach: preserving human dignity as a paramount principle .....	200

## Keywords

U.K. Children's Code – Empowerment – Convention on the Rights of the Child (CRC) – design discourse – Human Dignity

### 1. Introduction

Among the global challenges of our time, the protection of children in the digital environment represents one of the most urgent and complex tasks ever addressed in the present time, from a legal, social, economic and ethical point of view. According to recent data collected in research conducted by UNICEF, in fact, one-third of online users in Europe are under the age of 18 and numbers are destined to increase

in the coming years, in consideration of the long-term effects resulting from the Covid-19 pandemic<sup>1</sup>.

At the same time, it is a fact that the Internet “was not designed with kids in mind”<sup>2</sup>. The result is right in front of our eyes with countless new episodes where minors are daily victims of a distorted use of the web<sup>3</sup>. It should be noted, however, that in the last few years the awareness by the international institutions – in particular the European ones – and by the civil society as well, has increased evidently, leading to a series of initiatives launched to promote greater protection for minors and a better understanding of their rights<sup>4</sup>. In addition to representatives of institutions - national and international - a number of debaters were involved such as, among others,

---

<sup>1</sup> See, “Child rights and the 2030 Agenda for Sustainable Development in the context of the COVID-19 pandemic”, in [https://www.ohchr.org/sites/default/files/Documents/Issues/Children/ChildRights\\_2030Agenda.pdf](https://www.ohchr.org/sites/default/files/Documents/Issues/Children/ChildRights_2030Agenda.pdf).

<sup>2</sup> See, European Digital Rights, Age against the machine: the race to make online spaces age-appropriate, in <https://edri.org/our-work/age-against-the-machine-the-race-to-make-online-spaces-age-appropriate/>, September 4, 2024.

<sup>3</sup> See, National Society for the Prevention of Cruelty to Children (NSPCC), in collaboration with leading experts in academia on online child protection, published in November 2023, which outlines and exposes evidence on the risks and dangers present online for children and that emerged during the period 2017-2023 in the UK. The report focuses on the dissemination and use of child pornography as well as, more generally, the distorted use by platforms of the design features of websites frequented by children. Consider, among others, so-called dark patterns. The report can be found at <https://learning.nspcc.org.uk/media/ezjg0pbj/online-risks-children-evidence-review-main-report.pdf>; J. Bryce, S. Livingstone, J. Davidson, B. Hall, J. Smith, *Online risks to children: evidence review*, November 2023.

<sup>4</sup> Among the numerous ones, see EU Kids Online. This is an international research network whose goal is to improve the degree of knowledge and awareness among European children about opportunities, risks and safety in the digital environment. Through the use of a multidisciplinary approach, the project aims to map the online experience of children and parents, in constant dialogue with national and European policymakers and stakeholders. On this point, see D. Smahel, H. Machackova, G. Mascheroni, L. Dedkova, E. Staksrud, K. Ólafsson, S. Livingstone, U. Hasebrink, EU Kids Online 2020: Survey results from 19 countries. EU Kids Online, at <https://www.lse.ac.uk/media-and-communications/research/research-projects/eu-kids-online/eu-kids-online-2020>. Similarly, also in the European context, in May 2021 as part of the Better Internet for Kids initiative, a guide was published regarding best practices identified in some member states, Children's rights in the digital environment: moving from theory to practice, available at <https://www.betterinternetforkids.eu/documents/167024/200055/Best-practice+guideline+-+Childrens+rights+in+the+digital+environment+-+May+2021++v2+FINAL+CC+BY.pdf/f947d4f9-4ec4-49ae-5e2e-b6e9402c5fa2?t=1624532196598>. Most recently, on September 24, 2024, the United Nations approved the Global Digital Compact, in which fundamental rights are also reaffirmed in the digital dimension, with special attention given to children's rights. The overriding goal of the Global Digital Compact is to “strengthen legal and policy frameworks to protect the rights of the child in the digital space,” in <https://www.un.org/sites/un2.un.org/files/sotf-the-pact-for-the-future.pdf>.

organizations in defense of children, representatives of the academic world and, in part, also the digital industry (so-called stakeholders).

The core issue regarding the empowerment of children in the digital environment necessary implies a series of considerations about: parental responsibility, institutions' involvement, stakeholders' role and, mainly, the minors' voices.

While all these elements are specifically regulated in the Convention on the Rights of the Child (CRC) – which represents at present the most ratified international convention in the matter of children's rights and the legal framework of reference<sup>5</sup> – nevertheless, neither the international community and the others actors involved, seem to take the CRC into serious and concrete consideration when it comes to implement actual policies in favor of the minors' empowerment.

Moreover, the evident contrast between the law in the books and the law in action<sup>6</sup> - that is between the established rule and the operational rule<sup>7</sup> - is particularly sharp in the matter of the digital dimension. Even though the CRC Committee has clearly pointed out that children's rights fully apply also in the digital environment, resistances and oppositions of various nature make the goal of protecting and promoting children's rights very difficult to achieve<sup>8</sup>.

This article explores the benefits of adopting a child-centered approach in addressing the topic here presented, through the concrete example of the U.K. Age –

---

<sup>5</sup> The Convention on the Rights of the Child (CRC) was approved by the United Nations General Assembly in New York on November 20, 1989, and entered into force on September 2, 1990. To date, it is the international document that has received the highest number of ratifications by states, with the sole exception of the United States of America.

<sup>6</sup> J.L. Halperin, *Law in books and law in action: the problem of legal change*, 64 Me. L. Rev. 2011, p. 45; R. Pound, *Law in books and law in action*, 44 Am. L. Rev. 1910, p. 12; D. Nelken, *Law in action or living law? Back to the beginning in sociology of law* 1, 42 Legal studies 1984, pp. 157-174.

<sup>7</sup> Comparative law makes extensive use of this methodological approach. See, P.G. Monateri, *Morfologia, Storia e Comparazione. La nascita dei "sistemi" e la modernità politica*, in *Diritto: storia e comparazione. Nuovi propositi per un binomio antico*, Frankfurt, 2018, 267-290; R. Scarciglia, *L'Objetto Della Comparazione Giuridica (Objects and Legal Comparison)*, in R. Scarciglia (edited by), *Introduzione al diritto pubblico comparato*, Bologna, 1966, pp. 47-68; G. Ajani – B. Pasa – D. Francavilla, *Diritto comparato: lezioni e materiali*, Torino, 2018; A. Somma, *Giochi senza frontiere: Diritto comparato e tradizione giuridica*, 37:109 *Boletín mexicano de derecho comparado*, 2004, pp. 169-205.

<sup>8</sup> See, General Comment n. 25, <https://www.ohchr.org/en/documents/general-comments-and-recommendations/general-comment-no-25-2021-childrens-rights-relation>, CRC/C/GC/25, 2 March, 2021, "Children's rights in relation to the digital environment".

Appropriate Design Code, better known as the U.K. Children's Code<sup>9</sup>. The paper analyses the structure of the Code showing its strict connection with the CRC, also underlining how the way the Code's drafting process was developed and defined, contributed to its success. It then advances the argument that adopting a child-centered perspective means fully respecting the roles and prerogatives of all the actors involved, ultimately conveying to the empowerment of the minors and, therefore, of the whole collectivity.

## **2. The U.K. Children's Code in the prism of the CRC and of the design discourse**

The U.K. Children's Code is a code of conduct, consisting of 15 standards, mainly aimed at digital platforms offering online services targeting minors, which came into effect in September 2020 in the United Kingdom, drafted by the Information Commissioner's Office (ICO), the UK's independent data protection authority. The ICO is competent in "upholding information rights in the public interest, promoting openness by public bodies and data privacy for individuals and empowering people through information"<sup>10</sup>.

The Children's Code is a statute and, therefore, in the system of the English legal sources, it is part of the so-called legislation, or "the law created by the competent organs of the state and condensed into precepts expressed in written formulas"<sup>11</sup>.

---

<sup>9</sup> See, the U.K. Age Appropriate Design Code, known as Children's Code, enacted by the Information Commissioner Office in 2020, <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/introduction-to-the-childrens-code/>. See, *infra*, par. 2.

<sup>10</sup> <https://ico.org.uk/about-the-ico/our-information/our-strategies-and-plans/ico25-plan/>.

<sup>11</sup> G. Criscuoli, *Introduzione allo studio del diritto inglese: le fonti*, 2014, Torino, p. 411 ff. Although they are not as numerous as sources of judicial origin, as the A. notes, legislative sources also play a function "of primary importance, not only because of the original normative content they can have, but especially because of the sometimes decisive impact they can have on the life of the normative principles of case law." On the role statutes have occupied and still occupy in the hierarchy of English sources, see also, among others, T. Plucknett, *A Concise History of the Common Law*, 5th ed., Boston, 1956; M.S. Arnolds, *Statutes as Judgements: The Natural Law Theory of Parliamentary Activity in Medieval England*, 126 U. Pa. L. Rev., 1977, p. 329; C.K. Allen, *Law in the Making*, 7th ed., Oxford, 1964; U. Mattei, E. Ariano, *The common law model*, Turin, 2018, p. 233 ff.

With specific reference to the expression ‘code,’ a clarification should be made: indeed, this is not the same concept as the ‘code’ typical of civil law systems. As it is well known, in fact, there is no use in English law of the code in the same way as a general system of norms. However, just as in Italy not all law is codified, even in England some specific issues have been the object of a specific regulation, such as in the case of the UK Age-Appropriate Design Code<sup>12</sup>.

The Children's Code, therefore, will work as a reference for the courts - as, indeed, specified by the Code itself in the Executive Summary - when it comes to the protection and promotion of the rights of the child online, in a position, however, that is interstitial and of specialty with respect to common law in general.

As legal scholars remarked, “Despite the enormous amount of legislation produced, the most important part of our law remains common law [...]. Statutes are nothing more than addenda and errata to the book of common law and would have no meaning except in reference to common law [...]”<sup>13</sup>.

The Code is aimed at all companies offering online services (information society services - ISS) to which, potentially, minors could also have access (likely to be accessed), such as video games, entertainment applications, smart toys, etc. As expressly stated, the ultimate goal is to ensure protection for under-age users through proper design of the systems underlying the services offered and appropriate use of the data entered and circulating on the network.

---

<sup>12</sup> More generally, this can be traced to that activity of collection and arrangement which, technically, is called consolidation. On the distinction between codification and consolidation, see G. Criscuoli, cit., p. 16 ss., who points out, among the most typical aspects of the difference between these two techniques, that whereby “consolidation does not affect the binding value of judgments issued prior to the act of consolidation, as opposed to codification, which, on the other hand, eliminates the binding effect to judgments related to reformed rules.”

<sup>13</sup> W. Geldart, *Elements of English Law*, 1975, 80 ed., p.2. Geldart's words are also mentioned by A. Guarneri, *Lineamenti di diritto comparato*, 2022, p. 348. F. Pollock wrote «The best and most rational portion of English law is in the judge made law», *The Law Quarterly Review*, 1893, p. 106. On the historical relationship between common law and statutes, see also, C.K. Allen, *Law in the Making*, 7<sup>th</sup> ed., Oxford, 1964, *passim*, and more recently, A. Miranda, *Smoke gets in Euro-eyes: fusione e fissione del diritto comunitario*, in Liber Amicorum Luigi Moccia, edited by E. Calzolaio, R. Torino, L. Vagni, Roma TrE press, Roma, 2021, p. 389 ss.

More generally, the Code stems from the need to protect minors *within* the digital dimension, and not, instead, from the need to prevent them *from* accessing it<sup>14</sup>.

As previously mentioned, it consists of 15 standards, which are not merely technical requirements, but parameters to be used to design an adequate protection of the minors' data. The standards are: best interests, data protection impact assessments, age-appropriate application, transparency, detrimental use of data, policies and community standards, default settings, data minimization, data sharing, geo location, parental controls, profiling, nudge techniques (also known as dark patterns), connected toys and devices, online tools<sup>15</sup>.

In order to understand how a standard works, it is worth to analyze, as an example, the one related to the default settings in order to realize how each standard is the result of the balance between the enhancement of the child, the parental responsibility, the (preventive) control of the company offering the service, and the (eventual) later control of the sanctioning authority.

Standard number 7 on default settings imposes an obligation on the company offering the service, to define and guarantee - from the beginning - the most restrictive level of privacy, unless it can be demonstrated that a different, lower-level approach is necessary in order to pursue the best interests of the minor.

In the case, for example, of a video game, minors will start using the product without the need for a change, on their part, to obtain a more restrictive level of privacy (so that their data will not, for example, be used by third parties) because the platform has already done so, in this respect. Rather, and with an entirely reversed perspective, minors may be given the opportunity to change the default choice, for a less restrictive level, provided that, as clarified in the Code itself, they are put in a position to exercise their rights consciously, and are provided with all the information they need to

---

<sup>14</sup>See, <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/age-appropriate-design-a-code-of-practice-for-online-services/about-this-code/#code1>.

<sup>15</sup> For the specific of each standard, see <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/age-appropriate-design-a-code-of-practice-for-online-services/code-standards/>.

understand what the consequences of any change in these settings are, in terms of the use and circulation of their data<sup>16</sup>.

As it becomes quite clear, there is a strong connection between the standards and the CRC, connection also underlined by the same Executive Summary of the Code, when it explicitly declares that the Code is “rooted in the United Nation Convention on the rights of the child”. As a matter of fact, the entire structure of the Code responds to the logic that is proper to the Convention, namely that of the protection of the child as a *subject* fully entitled to rights, who is recognized, depending on the maturity and on the context, a progressive acquisition of autonomy in the decisions that affect him or her, according to the principle of the evolving capacities.

As it is well known, indeed, the CRC formally establishes the transition from a paternalistic conception, traditionally oriented towards the idea of the minor as an “object” of law, to a vision in which, on the contrary, as mentioned, the minor becomes a full “subject” of law. This change in perspective, specifically, is achieved, on the one hand, through the recognition of the individual traditional freedoms in terms of fundamental rights, granted to every human being by international treaties and here adapted to the specific situation of minors; on the other hand, through the introduction of a series of “new” rights closely linked to the peculiarities of the condition of minors, both within and outside the family unit.

Thus, with regard to the first aspect, the provisions of Articles 13 to 17 recognize the child's right to freedom of expression and thought, as well as freedom of religion, association, and the right to privacy. The Convention also emphasizes the right of access to information and the need for minors to have a variety of information

---

<sup>16</sup> “You can also use privacy settings to support the exercise of children's data protection rights (such as the rights to object to or restrict processing). And they can give children and parents confidence in their interactions with your online service, and help them explore the implications of allowing you to use their personal data in different ways”. See, <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/age-appropriate-design-a-code-of-practice-for-online-services/7-default-settings/>.

sources at both the national and international levels, especially those aimed at promoting their physical and spiritual well-being<sup>17</sup>.

The rights concerning the second aspect are more specific. They are aimed at protecting minors in certain situations (such as removal from their parents against their will, unless such removal is not in the best interests of the child)<sup>18</sup>, to ensure the principle of parental responsibility in the education and upbringing of the child<sup>19</sup>, and finally to protect the child from all forms of violence, throughout the period of custody by one or both parents or the legal representative<sup>20</sup>.

The Convention on the Rights of the Child, therefore, has opted for a reversal of the traditional view of minors as individuals, incapable of providing for themselves and, consequently, perpetually dependent on the decisions of others, elevating minors from a context of immobility and subjugation to a dynamic context in which, on the contrary, they can become protagonists of their own choices.

It is indeed in this perspective that Appendix B of the Code concretely refers to the principle of the evolving capacities. As a matter of fact, it expressly provides for the so-called *developmental stages*, indications addressed to online operators, that have the precise intent of guiding companies that offer services to minors, in the application of the standards themselves, according to the age ranges of the users they address.

---

<sup>17</sup> Artt. 13, 14, 15, 16 and 17 of the CRC about: freedom of expression, freedom of thought and conscience, religion, privacy, access to information and material from a diversity of national and international sources.

<sup>18</sup> See, art. 9 (1): “States Parties shall ensure that a child shall not be separated from his or her parents against their will, except when competent authorities subject to judicial review determine, in accordance with applicable law and procedures, that such separation is necessary for the best interests of the child. Such determination may be necessary in a particular case such as one involving abuse or neglect of the child by the parents, or one where the parents are living separately and a decision must be made as to the child's place of residence”.

<sup>19</sup> See, art. 18 (1): “States Parties shall use their best efforts to ensure recognition of the principle that both parents have common responsibilities for the upbringing and development of the child. Parents or, as the case may be, legal guardians, have the primary responsibility for the upbringing and development of the child. The best interests of the child will be their basic concern”.

<sup>20</sup> Art. 20 (1): “States Parties shall take all appropriate legislative, administrative, social and educational measures to protect the child from all forms of physical or mental violence, injury or abuse, neglect or negligent treatment, maltreatment or exploitation, including sexual abuse, while in the care of parent(s), legal guardian(s) or any other person who has the care of the child”.

Specifically, the Code identifies five age ranges: the pre-literate and early literacy (up to 5 years of age); that corresponding to the primary school years (6 to 9 years of age); the so-called transition years (10 to 12 years of age); early adolescence (13 to 15 years of age); and the so-called approaching adulthood (16 to 17 years of age). These are, however, indicative ranges since, as it says, "Children are individuals, and age ranges are not a perfect guide to the interests, needs and evolving capacity of an individual child. However, you can use age ranges as a guide to skills and behaviors a child might be expected to display at each stage of their development"<sup>21</sup>.

The Code's link to the Convention is further confirmed when it recalls firmly and explicitly the role of parents and family members in general, as well as the role of institutions.

As a matter of fact, the Code expressly states that the standards represent a support and help for parents to clarify and, possibly, solve a number of issues that arise whenever a child uses a digital tool such as, for example, in the so-called by default settings concerning privacy. Similarly, the standards also address the need for institutions to comply with the requirements of the Data Protection Act (DPA) of 2018<sup>22</sup>, which in turn transposes the European GDPR, and in particular from Recital No. 38.

Furthermore, the Code reinforces the so-called participatory rights<sup>23</sup> - that characterize the entire Convention - in the digital dimension, where it recognizes

---

<sup>21</sup>See, <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/age-appropriate-design-a-code-of-practice-for-online-services/3-age-appropriate-application/> .

<sup>22</sup> <https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted>. The Data Protection Act, which was finally approved on May 23, 2018, implements the European General Data Protection Regulation (GDPR). It is an updated version of the previous 1998 legislation, specifically drafted to address the challenges of the digital age. In particular, the new version focuses on the protection of so-called sensitive data and their greater protection, such as, among others, race, ethnic background, political opinions, religious beliefs, trade union membership, genetics, biometrics, health, sex life, or orientation.

<sup>23</sup> The use of the expression "participatory rights" can be ascribed to the Committee on the Rights of the Child, which has the task to monitor and promote the implementation of the Convention on the Rights of the Child in the legislation of member states. In particular, see Concluding observations Spain UN Doc. CRC/C/15/Add.28, 1995; Nicaragua UN Doc. CRC/C/15/Add.36, 1995; Germany U.N. Doc. CRC/C/15/Add.43, 1995, available on the official website of the United Nations. For a multidisciplinary analysis of participation rights, see A.B. Smith, *Interpreting and supporting participation rights: Contribution from socio-*

freedom of expression, thought, and religion; of privacy; of association; of access to information in the mass media (of course in the terms in which the Code operates); of gaming and entertainment (again, dropped into digital reality); of protection from economic, sexual, or other exploitation, as well as pertaining to the web . The key elements of the relationship between the standards and the UN Convention are, therefore, to be found in the *evolving capacities* of the child, the central role of the family and the equally indispensable role of institutions and stakeholders<sup>24</sup>.

In this perspective, another aspect which played a fundamental role in the success of the Code, pertains to the modalities chosen for the drafting of the Code itself. As a matter of fact, it is the result of a shared action between institutions, third sector organizations and representatives of the digital industry. It all started from the nongovernmental organization *5RightsFoundation*, founded by Baroness Beeban Keedron, a successful film producer and member of the House of Lords, in collaboration with academics and various stakeholders, who, in 2018, launched a strong campaign aimed at verifying, in concrete terms, the state of the art regarding the use, by minors, of digital tools and, at the same time, the (possible) measures taken by platforms for the access to the online contents by minors themselves.

The survey, part of an ongoing project, highlighted the real impact of the digital dimension on minors, particularly in the aftermath of the COVID 19 pandemic, under different profiles including, the relationships within the family unit, between the minors themselves inside and outside the school context, between the individual minor and the digital tool in relation to the use of social networks. The data collected shows a high level of datafication in the daily lives of children, and the substantial

---

cultural theory, in 10 The International Journal of Children's Rights, 2002, 1, 74. See, also E. Munro, *Empowering looked-after children*, in 6 Child and family social work, 2002, 1, 74. More recently, see

<sup>24</sup> M. Couzens, *Autonomy rights versus Parental Autonomy*, in AA.VV., The U.N. Children's Rights Convention: Theory meets Practice. Proceedings of the International Interdisciplinary Conference on Children's Rights, Intersentia, Oxford, 2007, pp. 420 ss. See, <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/age-appropriate-design-a-code-of-practice-for-online-services/about-this-code/>.

absence of measures aimed at effective protection in accordance with the principles set out in the UN Convention on the Rights of the Child<sup>25</sup>.

These findings represented the starting point for undertaking intensive lobbying - by 5Rights, child protection associations and representatives of the major digital industries, vis-à-vis Parliament - which led to the goal of drafting and approving, the Code.

### **3. The impact of the Code: concrete results**

The most immediate objection that could be made, and in fact is very often made, is that little or nothing has changed or will be able to change for minors accessing the net, despite the intentions and interventions put in place by the states or the international organizations. In this respect, it is useful to recall the report, published in May 2024 and compiled by 5Rights in collaboration with the London School of Economics (LSE) and the association Digital Futures for Children, entitled "Impact of regulation on children's digital lives," which analyzes the changes made by some digital platforms, mainly in Europe and U.K, in the period between 2017 and 2024, in the direction outlined by the Code<sup>26</sup>.

The report is the result of an investigation that involved an initial phase of data collection, through requests made directly to the platforms to provide the data; a second phase of reprocessing, referring to both the type of change and the period in which it was made.

The report focuses on the UK and European context and specifically considers the impact that the UK Age Appropriate Design Code, in particular, and to a much lesser extent the Digital Services Act, have had in terms of protecting minors in relation to privacy, security, and data protection.

---

<sup>25</sup> Research Report, Impact of regulation on children's digital lives, May 2024, [https://eprints.lse.ac.uk/123522/1/Impact\\_of\\_regulation\\_on\\_children\\_DFC\\_Report\\_May\\_2024.pdf](https://eprints.lse.ac.uk/123522/1/Impact_of_regulation_on_children_DFC_Report_May_2024.pdf).

<sup>26</sup> Impact of regulation on children's digital lives, Research report, May 2024. V. [https://eprints.lse.ac.uk/123522/1/Impact\\_of\\_regulation\\_on\\_children\\_DFC\\_Report\\_May\\_2024.pdf](https://eprints.lse.ac.uk/123522/1/Impact_of_regulation_on_children_DFC_Report_May_2024.pdf).

It should also be noted that the document also considers a series of other non-EU regulatory measures; however, as highlighted in the report itself, the data show that the majority of changes made by platforms occurred following the approval of the UK Code and, to a lesser extent, the EU directive<sup>27</sup>.

The most relevant changes seem to be concentrated in the 'by default' category, where there are the highest number of changes, made in 2021, to coincide with the Code's entry into force.

For example, Instagram (part of the Meta group) changed the initial setting of under-16 accounts from 'public' to 'private' as pre-defined; Google disabled, again as pre-defined, the application related to the history tracking feature.

Other changes affected, again in the by default category, the very management of the account on the platform: for example, Tik Tok disabled automatic notifications after 9 and 10 p.m. for minor users, and set 60 minutes per day as the maximum limit of video exposure for minors.

Changes are likewise recorded in the area of advertising, where, for example, Tik Tok provides a set of disclosures for users between 16 and 17 years old with regard to the operation of advertisement alerts, while it has disabled, by default, personalized alerts for all minor users.

Changes are likewise recorded in the area of advertising, where, for example, Tik Tok provides a set of disclosures for users between 16 and 17 years old with regard to the operation of advertisements, while it has disabled, by default, personalized alerts for all minor users.

In terms of security, the Tik Tok platform also shows that it is among the most active. In fact, for users under the age of 16, the option to send private messages with stranger users has been disabled, by default, while Instagram places an alert -

---

<sup>27</sup> Ofcom's *Children and parents: Media use and attitudes report* (2023) ([www.ofcom.org.uk/research-and-data/media-literacy-research/childrens/children-and-parents-media-use-and-attitudes-report-2023](http://www.ofcom.org.uk/research-and-data/media-literacy-research/childrens/children-and-parents-media-use-and-attitudes-report-2023)); Pew Centre's *Teens, social media and technology 2023* (<https://www.pewresearch.org/internet/2023/12/11/teens-social-media-and-technology-2023/>); and YPulse's 'These are European Gen Z's top social media platforms' ([www.ypulse.com/article/2023/06/13/we-these-are-european-gen-zs-top-social-media-platforms](http://www.ypulse.com/article/2023/06/13/we-these-are-european-gen-zs-top-social-media-platforms)).

“suspicious behavior” - next to the account of adult users for whom there is unusual interaction activity with accounts of underage users.

Another example worth mentioning is concerning a British platform offering online games with 60 million users, called Poki.

In early 2023, an investigation conducted by the 5Rights Foundation revealed that, despite being accessed by millions of users in the UK, many of whom were under the age of six, the Poki platform continued to commit a series of violations: it tracked children's activities by default; it geolocated and monitored users without their consent; it shared children's data with third parties, often for “unspecified purposes”; it used ‘nudge techniques’ (dark patterns), manipulating children and inducing them to reduce their privacy settings. Children's profiles, their precise geolocation, and detailed information about their gaming practices and habits were shared directly with more than 300 external companies, advertising and marketing companies, analytics companies, and data brokers located in the United Kingdom, the United States, and China.

Following a formal communication sent by 5Rights in March 2023, and eight months of subsequent consultations, the platform radically revised the design of its system to comply with the Age Appropriate Design Code.

The changes made include: changing the default settings to ensure the highest level of privacy; limiting cookies; replacing profiling-based advertising with contextual ads; disabling the geolocation feature; and revising the privacy policy to make it more understandable and accessible. It is worth noting that the company has decided to implement these measures for *all users*, without distinction between adults and minors, as required by standard no. 3 on age-appropriate application.

While we are aware that a key role has also been played by investigations and, at times, sanctions imposed by the relevant national privacy authorities, nevertheless, the emerging data appear comforting and seem to confirm that the path indicated by the UK Code is appropriate.

A further observation should be made with regard to the fact that the examples given—although they constitute a huge step forward, rarely represent the rule and, above all,

do not imply that all 15 standards are complied with and applied simultaneously by all the actors involved.

On this point, it should be remembered that one of the distinguishing traits of the Code, is precisely the fact that it has envisaged and constructed a mechanism that does not end with mere compliance with the standards by the companies, but provides for the active involvement, at the same time, of the child and the family, as well as, more generally, of the institutions. This ensures that all these actors contribute to its implementation, each for their own role and responsibility, so that the goal is achieved.

In this way, that much-feared “digital tsunami” Stefano Rodotà was talking about, is averted and, instead, a personal protection network is implemented, which, however, needs the involvement of all stakeholders<sup>28</sup>.

#### **4. Imitation and circulation of the Code: does it work?**

The affirmation of the UK Age-Appropriate Design Code in the United Kingdom has sparked particular interest also overseas, both in Europe and in North America. In fact, since 2021, there has been a significant spread of the British Code, along with scattered instances - mainly in Europe and the US - of imitation, prompting some brief considerations on the circulation, imitation, and reception of models.

Without any claim to delve into a topic that has been addressed by leading scholars<sup>29</sup>, one wonders whether – in fact – the hypothesis of the English Code could fall within

---

<sup>28</sup> S. Rodotà, *Il Diritto di avere diritti*, Bari, 2014, p. 337, who underlines how data, particularly personal data, are “attratti nell’orbita onnivora del sistema delle imprese e degli organismi di sicurezza”.

<sup>29</sup> A. Watson, *Legal transplants: an approach to comparative law*, Edinburgh, 1974; Id., *Law and legal change*, 38 Camb. L. J., 1978, p. 313.; Id., *TwoTier Law, an approach to law making*, Int. & Comp. L. Q., 1978, p. 552; Id., *Legal change: sources of law and legal culture*, 131 Un. of Pennsylvania L. Rev., 1983, p. 1121. On some critics to Alan Watson’s work, see O. Kahn-Freund, *Book Review, Legal Transplants*, 91 L.Q.R., 1975, p. 292; W. Twining, *Diffusion of law: a global perspective*, Journal of Legal Pluralism, 2004, p. 49; Id., *General jurisprudence: understanding law from a global perspective*, London, 2009; P.G. Monateri, *The Weak Law: Contaminations and Legal Cultures (Borrowing of Legal and Political Forms)*, 2008, on line [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=1300298](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1300298). On formants and circulation of models, R. Sacco, *Legal Formants: A Dynamic Approach to Comparative Law*, I, *The American Journal of Comparative Law*, 1991, pp. 39, e 34 and II, p. 343; R. Sacco, A. Gambaro, *Sistemi Giuridici Comparati*, Torino, 1996, 4; R. Sacco, *Circolazione e mutazione dei modelli giuridici*, Digesto civ., II, Utet, Torino, 365.

the phenomenon whereby, in sectors that present very similar issues and problems to be resolved. The acquisition of models already tested in other contexts would facilitate a 'virtuous' process of reforms<sup>30</sup> and, in a certain way, could convince national and international actors to adopt such similar models<sup>31</sup>; thus also achieve a certain level of 'spontaneous harmonization' of protection standards and fundamental principles<sup>32</sup>, obviously on the condition that the phenomenon is framed taking into account the historical and evolutionary differences and the context of the individual systems and, therefore, their legal traditions.

As it has been observed, in fact, '*the circulation and imitation of the model does not depend so much on the intrinsic qualities of the legal system or the model being imitated, but rather on the strategies and problems of the system that is imitating*'<sup>33</sup>.

In this regard, the drafting of the English Code has certainly helped to rekindle the interest of the international community and, consequently, of national legislators, on the matter of child protection in the digital world, offering a new perspective to address the issue, considering, on the one hand, the concrete profile that characterizes

---

On the dialogue between Sacco and Watson, see S. Ferreri, *Asonanze transoceaniche. Tendenze a confronto*, in 1, Quadrimestre, rivista di diritto privato, 1993, p. 179; U. Mattei, *Why the wind changed. Intellectual leadership in western law*, 42, Am. J. Comp. Law, 1994, p. 195; A. Watson, *From legal transplants to legal formants*, 43 *American Law Journal of Comparative Law*, 1995, 3, 469; P.G. Monateri, *Black Gaius*, 51 *Hastings L.J.*, 2000, p. 510; M. Graziadei, *Comparative Law, Transplants, and Receptions*, in M. Reimann e R. Zimmermann (edited by), *The Oxford Handbook of Comparative Law*, 2. ed., Oxford, 2019, p. 442 ss; AA.VV., *Esperienze giuridiche in dialogo. Il ruolo della comparazione*, M. Graziadei and A. Somma (eds), Roma, 2024, passim.

<sup>30</sup> A. Dondi, *Comparazione oggi. Brevi (e molto limitate) impressioni dal côté processuale*, in A. Somma, V. Zeno-Zencovich (edited by), *Comparazione e diritto positivo. Un dialogo tra saperi giuridici*, Roma, 2020, p. 333 ss.

<sup>31</sup> M. Graziadei, *Legal Transplants and the Frontiers of Legal Knowledge*, in *Theoretical Inquiries in Law*, 2009, (10) 2, p. 693. See, also, in the matter of environmental protection, B. Pozzo, *Modelli notevoli e circolazione dei modelli giuridici tra in campo ambientale: tra imitazione e innovazione*, in *Studi in Onore di Antonio Gambaro. Un giurista di successo*, Milano, 2017, p. 351.

<sup>32</sup> G. Benacchio, *Diritto privato della Unione Europea*, Milano, 2016, p. 131 ss, regarding the phenomenon of the circulation of rules and legal models in Europe. Specifically in the European legal context, the Author underlines that this analysis represents a very useful tool in order to understand the role exercised by the so called 'competition among models' in the legislative process. See, also, A. Plaia, (edited by), *La competizione tra ordinamenti giuridici. Mutuo riconoscimento e scelta della norma più favorevole nello spazio giuridico europeo*, Milano, 2007; A. Zoppini, *La concorrenza tra ordinamenti giuridici*, Roma, 2004.

<sup>33</sup> A. Miranda, *Trapianti giuridici, circolazione dei modelli e persistenza della norma: l'insegnamento di Alan Watson*, in A. Miranda, *Diritto e tradizione. Circolazione, decodificazione e persistenza delle norme giuridiche*, Palermo, 2004, p.17.

the standards and, on the other, the involvement of the many actors directly affected by this issue. If we look at what has happened since the Code was issued in the United Kingdom, we can see a series of related or influenced initiatives, such as the approval of similar Codes in the state of California and other US states, as well as in the Netherlands, the publication of the UN General Comment n. 25 specifically referring to the rights of children in the digital dimension – directly inspired by the English Code – together with similar initiatives by the EU institutions on the subject.

On the other hand, despite the general agreement on the rationale and intentions of the original English model, an overview of these initiatives also reveals a series of differences and difficulties related, among other things, to environmental, political, and cultural factors which, to varying degrees, affect the reception of the Code model.

It is the case of the California Age-Appropriate Design Code (CAADC), approved on September 15<sup>th</sup> 2022 by the state Assembly. The CAADC is inspired by the UK Age-Appropriate Design Code and is primarily aimed at all companies that offer online services that are likely to be accessed and used by minors.

This is the first piece of legislation in the United States that is directly inspired by the *by design* approach; it shares the general structure of the UK Children's Code, from which it borrows the indication of the standards in a similar way, but at the same time differs from it in some respects.

The analysis of the Californian legislation must necessarily take into account two areas of investigation: the first with respect to the federal legislation on the privacy of minors currently in force; the second with respect to the British Code. Both are significant in order to fully understand the main characteristics of the CAADC.

Regarding the federal legislation, the Children's Online Privacy Protection Act (COPPA) which regulates the protection of the privacy of minors, has been recently amended after an intense debate in Parliament, aimed at strengthening the protection of minors in relation to the introduction of new technologies. In this regard, a number of proposals for reforming COPPA – known and ultimately conveyed in the amendments known as COPPA 2.0 – have been put forward, starting in 2023, which

aim to extend the protection of minors online, particularly concerning the processing of their data by digital platforms<sup>34</sup>.

At the same time, another bill has been introduced (but still not passed into legislation) — the Kids Online Safety Act (KOSA) — which requires digital platforms to exercise a so-called duty of care, i.e., the obligation to implement a series of reasonable measures, mainly in terms of protecting minor users from the now very frequent phenomenon of cyberbullying. Moreover, it has to be observed that at the moment this paper is written, a comprehensive package has been introduced to the Senate — namely KOSPA (Kids Online Safety and privacy Act)<sup>35</sup> which includes both KOSA and COPPA 2.0. The bill, tough, languished for quite some time in the House of Representatives, due to the reservations of the Republican party and has not been approved yet. The main debate being around the notion of ‘duty of care’ and the recipients of this duty, also in consideration of the numerous ‘interventions’ by the actual administration aimed — *de facto* — at diminishing the duty of the (big tech) companies to protect minors online.

In the meantime, it is worth noting that, with regard to the subjective scope of application, while the text of the federal legislation previously in force (COPPA) considered only persons under the age of 13 to be minors, a limit also provided for in the European General Data Protection Regulation (GDPR), the new COPPA 2.0 (but not the KOSA proposal neither the KOSPA) adopts — albeit limited to the case of targeted advertising — a broader concept of a minor, even if not yet in line with that provided for by the UN Convention and the English Children's Code — *i.e.*, an individual under the age of 18 — which in turn is also provided for by the text of the California Code.

The new COPPA 2.0 amendments, in fact, sets the limit at 16 years of age, with a view to also including the adolescent age group that was previously excluded. Moreover, the new name of COPPA 2.0, namely the Children and Teens' Online Privacy Protection Act, would seem to confirm this choice.

---

<sup>34</sup> On June 23, 2025 the amendments went into effect, while the Federal Trade Commission finalised them in April 2025. The compliance deadline for companies is April, 2026. See the FTC official web page.

<sup>35</sup> See, <https://www.congress.gov/bill/118th-congress/senate-bill/2073>.

Another important issue that will have to be addressed, and which is likely to be the subject of heated debate, especially between more conservative and more progressive groups, is that of parental consent.

While the federal texts both of COPPA and of COPPA 2.0 are based precisely on the latter, *i.e.*, the necessary authorization of parents for minors to use online services (with poor results, however), the Californian text, adopting the rationale of its British counterpart, which in turn refers to the principles of the UN Convention on the Rights of the Child, embraces a different idea of ‘protection’, aiming at pursuing the best interests of minors through a series of requirements intended primarily for commercial operators and only secondarily for family members, with a view to gradually empowering all those involved.

With respect to the analysis of the British Code, it is necessary to reflect on the general structure of the two codes of conduct and, in particular, on the premise from which each of them originates and develops.

While the British Code, as previously mentioned, is based on and refers to the principles and rights contained in the UN Convention on the Rights of the Child (it is rooted in the UN Convention), the CAADC is a separate piece of legislation that, in general terms, refers to the best interests of the child. The CAADC obviously lacks any link to the Convention, given that the United States is the only country in the world that has never ratified it. This shortcoming gives rise to two considerations.

On the one hand, it indicates that the CAADC lacks the foundation and set of principles which, when interpreted as a whole, represent some of the key elements for a new and different conception of the child, which underpins the Convention itself and which play an important role, as seen in the English case, in the implementation of the standards contained in the Code. The notion of best interests, as regulated by Article 3 of the Convention, is, in fact, a tool that must be coordinated with the rest of the provisions in order to affirm the other principles, including that of evolving capacities.

On the other hand, it prompts reflection on the interpretation of the concept of best interest in the US legal framework. In this regard, it should be noted that this principle became established in American family law during the 19<sup>th</sup> century, in the context of

custody cases in divorces. Outside its original scope — in which it has been repeatedly criticized for its vagueness — it has found effective recognition in state legislation, especially in matters of adoption, but not the same clarity in the jurisprudence of the Supreme Court, which has shown a fluctuating orientation on several occasions<sup>36</sup>.

In fact, in 2015, in the well-known case of *Hobergefell v. Hodges*<sup>37</sup>, the judges recognized the right to marriage for same-sex couples, also in consideration of the need to safeguard the best interests of minors within the family unit, at the same time, in a series of other cases, the Court gave priority to the concrete assessment of the best interests of the child over other absolute legal presumptions, *i.e.*, it considered that the best interests must in any case be weighed and considered in relation to other responsibilities, primarily those of parents and public authorities<sup>38</sup>.

In this respect, it is once again necessary to ‘read’ the issue taking into account the context in which it arises and, certainly, in the case of the United States, the constitutional balance between federal and state power in matters of family relations has a considerable impact on the limits and connotations of this principle.

In relation to the concept of ‘best interests’, it is therefore appropriate to refer to the report drawn up by the 5Rights Foundation (the association that promoted the UK Children's Code) and the London School of Economics, published in March 2024<sup>39</sup>,

---

<sup>36</sup> L.M. Kohn, *Tracing the foundations of the best interests of the child standard in American jurisprudence*, in *Journal of Law and Family Studies*, 2008, p. 358 ss.; C. Breen, *The Standard of the best interests of the child: a western tradition in international and comparative law*, The Hague, 2002.

<sup>37</sup> *Hobergefell v. Hodges*, 35 S.Ct. 2584 (2015) in <https://supreme.justia.com/cases/federal/us/576/14-556/case.pdf>.

<sup>38</sup> *Flores v. Reno*, 507 US 292 (1993), in <https://supreme.justia.com/cases/federal/us/507/292/case.pdf>, in the matter of foreign unaccompanied minors, it was stated that “a venerable phrase familiar from divorce proceedings», is a proper and feasible criterion for making the decision as to which of two parents will be accorded custody. But it is not traditionally the sole criterion – much less the sole *constitutional* criterion – for other, less narrowly channeled judgments involving children, where their interests conflict in varying degrees with the interests of others. [...] So long as certain minimum requirements of child care are met, the interests of the child may be subordinated to the interests of other children, or indeed even to the interests of the parents or guardians themselves. [...] The best interest of the child is likewise not an absolute and exclusive constitutional criterion for the government’s exercise of the custodial responsibilities that it undertakes, which must be reconciled with many other responsibilities».

<sup>39</sup> S. Livingstone, N. Cantwell, D. Özkul, G. Shekhawat, B. Kidron, *The best interest of the child in the digital environment*, March 2024, in <https://www.digital-futures-for-children.net/best-interests>.

entitled 'The best interests of the child in the digital environment', which clarifies the scope and meaning of this expression, which is often abused and misused by companies offering online services to minors.

The research, in fact, reiterates that the continuous development of legislation and regulations on the protection of children's rights, both nationally and internationally, must be matched by equal caution and attention on the part of states and commercial operators in the use of the 'language' of children's rights. In other words, it is not enough to include the expression 'best interests' in order to have fulfilled and effectively followed through on the pursuit of the best interests and protection of the child. The reference to best interests, as well as to other rights, implies, as has been expressly and repeatedly stated, a reference to the entire Convention and, therefore, to the principles on which it is based.

A key passage concerns the United States: the report acknowledges that most tech companies are based in this country, the only one that has not ratified the UN Convention on the Rights of the Child.

However, the US remains a signatory to the Convention, which means that it is still obliged not to act in contravention of it. This becomes particularly important when one considers that the digital services offered by US companies have an impact on the lives of minors all over the world, or almost all over the world.

In this sense, the CAADC seems to have taken on board the message contained in the report, effectively placing itself at the forefront of both the federal Children's Online Privacy Protection Act (COPPA and the amendments) and the failure of the U.S. to ratify the CRC. The CAADC has clearly chosen the British Code as its model: the structure, the identification of standards, and even the name of the code of conduct are direct imitations. Curiously, however, the CAADC refers at the outset to the UN Convention in relation to the need to protect minors in all aspects of their lives.

However, as has been repeatedly pointed out, the federal government's failure to transpose the directive means that for this legal system, of reference to a context – that in which the Convention matured and developed – which represents a more complex and composite reality, made up of legal, cultural, and social elements, of a

sensitivity built up over time by the doctrine and the jurisprudence, which have evolved and cannot be replaced simply by inserting the expression 'best interests.' One need only think of the General Comments drafted annually by the UN, which have, from the outset, addressed issues that are crucial to the affirmation of children's rights.

This overview would seem to reveal a tension between the concept of best interest, which has become established over the years, particularly in the case law of the Supreme Court, and that expressed in both the Californian Code and the English Code. In the case of the Code approved in California, in particular, there is a clear need and, at the same time, a difficulty for the state legislator to reconcile the British view, which considers this principle as 'paramount', in line with the UN Convention, with the more 'relativized' view expressed by the courts, as mentioned above. The outcome is not yet clear, as it will be the judges who determine its limits and content.

Other differences between the English Code and the CAADC concern the processing of children's data and the data protection impact assessment, which in the case of the English Code are influenced by the requirements of the GDPR, in the matter of possible harms to rights and freedoms, while in the Californian text are generally referred to as 'material detrimental'.

In light of the above, when comparing the federal legislation on the one hand and the English model on the other, from a more general point of view, it is clear that, unlike the English Code, the Californian text is part of a regulatory and institutional context which seems more complex in certain respects. This is not only because of the presence of the federal level of legislation on the subject but also, and above all, because of the difficulty of balancing the protection of minors with other constitutionally protected freedoms. In particular, as far as we are concerned here, freedom of expression, which, as is well known, is protected at the constitutional level by the First Amendment, emerges in this specific case in its 'multi-directional' nature. The difficulty lies precisely in finding a balance between freedom of expression and self-determination of minors, freedom of expression of platforms and their users, and the duty of control and possible intervention by public authorities.

In the specific case of the California Age-Appropriate Design Code, it should be noted that in September 2023, the Federal District Court for the Northern District of California issued a preliminary injunction suspending the Code, as it was deemed contrary to and detrimental to the First Amendment. In turn, the California Attorney General filed an appeal arguing that the content of the law concerns the protection of minors online and does not infringe on freedom of expression or, even less so, free enterprise. Meanwhile, academics, politicians, representatives of child protection organizations, and attorneys general (bipartisan) have filed a document in support of the CAADC text (amicus brief)<sup>40</sup>, taking a clear stance in favor of the Code. To date, the decision of the 9<sup>th</sup> Circuit is pending.

A detail that should not be overlooked in this case is that the district court's injunction was issued in response to an appeal filed by Net Choice<sup>41</sup>, a national association that brings together some of the most influential online platforms. To get an idea of the organizations represented, among them are TikTok, Amazon, Meta, Yahoo, Google, and Airbnb, to name just the best known. As is easy to imagine, the interests protected and pursued by Net Choice are certainly different (if not in conflict) with those set out in the CAADC.

In this regard, there is another significant difference with the English Code. As has been mentioned before, the latter is the result of a shared process – from the outset and throughout the drafting process itself – between numerous and diverse stakeholders, including representatives of the digital industry. This does not mean that the conflicts in terms of interests pursued have been completely resolved, but certainly the involvement of all stakeholders from the outset has made it possible to better understand their respective positions and demands.

---

<sup>40</sup> V. Amicus Brief, <https://accountabletech.org/statements/broad-group-of-advocates-and-experts-file-amicus-briefs-countering-big-techs-attack-on-landmark-california-law-protecting-kids-online/?cn-reloaded=1>. See, also, the remarks by Daniel Solove, one of the leading experts in privacy, <https://teachprivacy.com/first-amendment-expansionism-and-californias-age-appropriate-design-code/>.

<sup>41</sup> *NetChoice, LLC, v. Rob Bonta*, Attorney General of the State of California. Order Granting motion for preliminary injunction. V. <https://storage.courtlistener.com/recap/gov.uscourts.cand.406140/gov.uscourts.cand.406140.74.0.pdf#page=2>.

In this respect, the provisions of the Children's Advisory Panel (CAP)<sup>42</sup> and periodic monitoring by the UK Information Commissioner's Office have proved particularly appropriate, as they help to create a more collaborative climate and, above all, ensure that the actual recipients of the regulation are involved in the regulatory process. Perhaps a similar strategy could have been implemented in the case of the Californian legislation.

However, the setback experienced by the CAADC has not discouraged other states, which, following California's example, are approving very similar codes. Following California's legislative initiative, other state assemblies have begun a similar process, approving texts more or less inspired by the California Age-Appropriate Design Code. Each of these has highlighted different aspects in their final or pending versions. An emblematic example of what has been said previously, is offered by the state of Utah, where the legislator's choice is characterized by an approach that is opposite to the British and Californian ones.

In fact, the state government has opted for so-called 'parental consent': this means that minors under the age of 18 must obtain parental authorization to use any social media. The initiative has raised more than one concern: firstly, because there is already federal legislation (the Children's Online Privacy Protection Act – COPPA) which, as mentioned, requires parental consent, and which has not produced the desired effects (given the amendments); secondly, because this choice confirms the evident desire to move away from the English Code model, which, as mentioned, is based on the idea of gradually recognizing a growing level of autonomy for minors. In this way, any decision is left to the parents, effectively nullifying the original idea behind the Code.

From this point of view, the distinctly conservative cultural tradition that characterizes this state's approach to family law, including parent-child relationships, probably plays a role. As is well known, the state of Utah is traditionally linked to the religious

---

<sup>42</sup> Starting with the first draft of the UK Children's Code drawn up in 2019, the Children's Advisory Panel (CAP) was established to coordinate the various 'souls' of the Code: minors, families, non-governmental organizations, and representatives of the digital industry. For example, UKIE, the association that brings together online game providers, is part of this panel. By holding regular sessions, the aim is to create and maintain genuine engagement and ensure that the Code is a successful outcome. See <https://ico.org.uk/about-the-ico/what-we-do/background-to-the-children-s-code/children-s-advisory-panel-cap/>.

doctrine of the Mormon group, a clear example of the hegemony of religious tradition as a model of social organization<sup>43</sup>.

In the case of Vermont and Minnesota, instead, the choice has been to align, generally, to the CAADC and, therefore, to the UK Code<sup>44</sup>.

One consideration that can be drawn from the above is that the English Code model is certainly circulating in the United States, albeit with different methods, nuances, and applications. The failure of the US to ratify the UN Convention plays a role in these different modes of reception, but it must be said that, in the case of the North American states, the framework of approved regulations shows a strong dependence on cultural factors, traditions, and, in particular, the role (*rectius* influence) of various stakeholders, as the Net Choice case has clearly highlighted.

While this paper does not focus specifically on the international and the European initiatives on this matter, that require an investigation *ad hoc*, it is of course worth remembering that the UK Code's influence is clearly evident in the General Comment n. 25 issued by the CRC Committee. Without going into details, it is very well known that this Comment is the result of a series of consultations among different groups of actors among which the 5Rights Foundation. Useless to say that the vision embedded by this association played a significant role in the drafting process of the Comment<sup>45</sup>.

Among the EU initiatives, the BIK+ strategy and of course the project for a European Age-Appropriate Design Code, represent an important step by EU institutions in the desired direction, as already seen in the British and US experiences, of protecting and promoting children's rights in the digital world.

---

<sup>43</sup> The reference here is to the very well-known classification in legal families by U. Mattei and P. Monateri, *Introduzione breve al diritto comparato*, Padova, 1997.

<sup>44</sup> V. <https://mgaleg.maryland.gov/2024RS/bills/hb/hb0603T.pdf>; <https://www.house.mn.gov/comm/docs/2hIcmA4QN0K9KVMGRvzBpw.pdf>.

<sup>45</sup> «The Comment is a culmination of three years of work during which 5Rights Foundation, supported the Committee on the Rights of the Child», in <https://5rightsfoundation.com/our-work/childrens-rights/uncrc-general-comment.html>.

Presumably, the EU Code should be supported by the rules contained in the GDPR and the principles contained in the UN Convention. Given that all EU member states have ratified it, this should – hopefully – be the legal framework of reference.

On the other hand, it should also be remembered that, in the meantime, there have been numerous legislative interventions by EU institutions in the field of digital technology (in the broad sense of the term), from the best-known regulation on artificial intelligence to the approval of the Digital Services Act<sup>46</sup>. All these pay particular attention to the more general protection of fundamental individual rights, with references to the European Charter of Rights, and this is a feature that has generally characterized the process of discussion, drafting, and approval in this specific area<sup>47</sup>.

Therefore, the future EU Code of conduct should have the task of providing concrete protection (in the sense intended by the Convention) and, at the same time, promoting the rights of minors online, bringing as much uniformity as possible to a framework which, although rich in valuable initiatives, still appears to be very fragmented and uneven overall. It is worth remembering that The Netherlands has already approved, in 2021, the *Code voor Kinderrechten*<sup>48</sup>, expressly referring to the British Children's Code. The Dutch text contains guidelines for companies offering online services that are also accessible to minors, which refer to the principles of the UN Convention and require the adoption of a series of behaviors inspired by the by design approach.

---

<sup>46</sup> <https://data.consilium.europa.eu/doc/document/PE- 49-2023-INIT/it/pdf>, par. 8, 56 and 101.

<sup>47</sup> This is not the place to examine the stages that led to the approval of the final text of the regulation on artificial intelligence, but it should be noted that many of the difficulties encountered concerned precisely the relationship between fundamental rights and artificial intelligence and the limits – if any – that should be set. There have been many recent contributions published on the subject. I will limit myself to citing the reflections of V. Zeno-Zenovic, *Artificial intelligence, natural stupidity and other legal idiocies*, *MediaLaws*, 2024, in <https://www.medialaws.eu/rivista/artificial-intelligence-natural-stupidity-and-other-legal-idiocies/>, who reminds us, if we had ever forgotten, that, regardless of all possible considerations about which approach is best for regulating technology, it is always and only human beings who enter data into the machine and decide what data to enter.

<sup>48</sup> [https://codevoorkinderrechten.nl/wp-content/uploads/2021/03/20210311\\_Code-voor-Kinderrechten\\_v1-1.pdf](https://codevoorkinderrechten.nl/wp-content/uploads/2021/03/20210311_Code-voor-Kinderrechten_v1-1.pdf).

More generally, the success of a (possible) European Age-Appropriate Design Code seems to be linked to the ability of EU institutions to create - as it has been the case in the UK since the drafting process - the optimal conditions for the various stakeholders to participate in its drafting. From this perspective, a bottom-up approach, as was the case with the Common Core project<sup>49</sup>, would be preferable.

This approach, indeed, aims to identify possible common responses and to exclude, instead, intervention imposed from above, could in fact prove to be more suitable for interpreting the needs of the community context.

Otherwise, the project would remain a dead letter or, worse still, could be relegated - like other initiatives - to a purely stylistic-doctrinal exercise.

---

<sup>49</sup> Originally, as is well known, the *Common Core* project was inspired by an idea of Rudolph Schlesinger, who conducted research on contracts at Cornell University in 1960. V.R. Schlesinger, *Formation of Contracts: a Study of the Common Core of Legal Systems*, New York, 1969, *passim*. The Common Core of European Private Law initiative, led by professors Mauro Bussani and Ugo Mattei as editors of the project, draws inspiration from this research and, in particular, from the methodology on which it is based: the so-called factual approach. The two editors combine this with Rodolfo Sacco's theory of formants, thus arriving at the so-called 'common core method', whose purpose is 'to unearth the common core of the bulk of European Private Law [...] The search is for what is different and what is already common behind the various private laws of European Union Member States [...] Such a common core is to be revealed in order to obtain at least the main lines of one reliable geographical map of the law of Europe.' On this point, see M. Bussani, U. Mattei, The Common Core Approach to European Private Law, in 3 *Columbia Journal of European Law*, 1997-1998, p. 339; M. Bussani, U. Mattei, Preface: the Context, in Bussani and Mattei, The Common Core of European Private Law, 2002, pp. 1-8. The Common Core project has developed along multiple lines, including that relating to the area of family law. The operational unit that carried out the research in this area applied this methodology to some of the most relevant aspects of family law, such as those relating to the division of assets between partners; *support rights and duties; administration and disposition of joint estate; dissolution of joint estate; dissolution of the relationship; family house*. The questionnaires submitted to the national rapporteurs, in fact, drawing directly on Schlesinger's project, are in no way intended to favor one system over another or, worse still, to hide the differences between the various legal systems, but rather to "map eventual common practical solutions, despite the letter of a civil code or statute's rule could provide differently." In the Common Core perspective, the scenario for the transnational lawyer, who approaches family law of different European legal systems, is that of a traveler compelled to use a number of different State's maps, each one containing (quite often) misleading information. The CC method tries to correct those misleading pieces of information, not forcing the actual diverse reality of the law within one single map to attain uniformity, but presenting a complex situation in a reliable way. A. Pera, *Searching for a common core of family law in Europe*, 1 *Opinio Juris in Comparatione*, 2018, p. 58 ff.

#### **4. A child centered approach: preserving human dignity as a paramount principle**

This brief analysis reveals a fact worth considering: a system where the responsibility for the use of a service or product likely to be accessed by minors is shared between the minors themselves, the family, the institutions, and the company offering the service, it is a system that guarantees not only the protection of minors, but, as we have seen with the Code standards, the promotion of their rights, since it fits fully into the concept of the evolving capacities contained in the CRC. Therefore, this system provides the minor with the tools to deal with the digital dimension, in a conscious and healthy way, in order to benefit from it as much as possible. The premise, let's remember, is to *encourage* aware use, not prohibit it.

From this perspective, therefore, precisely the empowerment we mentioned at the beginning is realized. This approach, authentically based on the principles of the CRC, clearly expresses another fundamental choice: the commitment to protect the *dignity* of the person, a prerequisite for any legal system, even more so considering vulnerable subjects as minors. As a matter of fact, the lesson we can draw from the UK Code is that a child-centered approach can be realized only if, at the same time, we take into consideration the value of human dignity.

This concept, as a matter of fact, in the context of the so-called disruptive technologies, proves to be decisive in preserving the autonomy of the individuals who make up the family unit. As it has been highlighted, *dignity* becomes the guiding principle and the criterion in the relationships between parents and children, between the family and institutions, and even with stakeholders themselves. The protection of human dignity is pragmatically oriented shaping the relationship between the minor and the parents and the duality parental responsibility /control *versus* the self determination of the minor.

In the analysis carried out with reference to the English model, the principle of dignity, in its various forms, certainly represents a recurring, shared, and therefore paramount value. More than any other, dignity is capable of overcoming the undeniable differences between the legal systems, since it is, on closer inspection, a value common to the Western legal tradition and which, therefore, from the point of view of the circulation of models, could also facilitate the acceptance of similar solutions in a future perspective of spontaneous harmonization.

Only doing so, we will truly protect the *person*, made of – as Stefano Rodotà reminded us of – a “corpo elettronico” and of a “corpo fisico”: two faces of the same medal, complementary, but without the first prevailing on the other<sup>50</sup>.

---

<sup>50</sup> S. Rodotà, cit., 2014.



3. The Digital Contract: New Challenges.....	207
4. The Minor in the Digital Contracts: Critical Issues .....	210
5. Protection and Empowerment .....	212
6. Prospective Outlook: What Role for Private Law? .....	214
7. Towards a Digital Private Law for Childhood .....	215

## Keywords

Contractual Capacity – Digital Private Law – Minors’ Autonomy – Consumer Protection – Algorithmic Contracting

### **1. Minors, Contracts and Technology: at the Origins of a New Systemic Conflict**

The convergence between contract law, digital technologies and the evolving status of minors generates a structural tension within private law: traditional civil law categories are confronted in markets designed to bypass awareness and negotiation. This tension is not merely doctrinal but systemic, calling for an ontological redefinition of the contract in the digital age.

The issue of contractual autonomy for minors in the digital environment raises a dual normative concern: on the one hand, there is a clear need to ensure effective protection against abuse<sup>1</sup>, manipulation<sup>2</sup>, and excessive commercial exposure<sup>3</sup>; on the other hand, it is equally important to recognise and promote a gradual legal self-

---

<sup>1</sup> Sonia Livingstone and Amanda Third, ‘Children and young people’s rights in the digital age: An emerging agenda’ (2017) 19 (5) NMS 657.

<sup>2</sup> Queennette Odudu, ‘Technological Solutions for Protecting Children From Online Predators: Current Trends and Future Directions’ (2024) SSRN 2, 11.

<sup>3</sup> Jenny Radesky, Yolanda Reid Chassiakos, Nusheen Ameenuddin and Dipesh Navsaria, ‘Digital Advertising to Children’ (2020) 146 (1) AAP 1, 3.

determination of minors<sup>4</sup>, in line with the evolving capacities principle set forth in the United Nations Convention on the Rights of the Child<sup>5</sup>. Private law is thus confronted with the task of reassessing its traditional categories—such as legal capacity, consent validity, and contractual liability<sup>6</sup>—in light of the specificities of digital interactions and the increasingly active role of minors within the digital ecosystem<sup>7</sup>.

This convergence reveals a structural misalignment between the normative premises of classical private law—such as informed consent, symmetrical negotiation, and relational reciprocity—and the realities of algorithmically mediated, opaque, and unilaterally imposed digital contracting. When these dynamics intersect with the specific vulnerabilities of minors, the contract becomes a site of systemic legal conflict: not merely an exception or anomaly, but a disruptive phenomenon that calls for an ontological redefinition of key civil law categories.

## 2. Capacity and Contractual Autonomy of Minors

In civil law systems such as the Italian and German ones, legal capacity constitutes a fundamental prerequisite to be able to fully exercise own private autonomy.

Article 2 of the Italian Civil Code establishes that full legal and contractual capacity is acquired upon reaching the age of majority, subject to specific exceptions for acts of ordinary administration or for emancipated minors<sup>8</sup>. This framework reflects a

---

<sup>4</sup> Yves Poulet, ‘e-Youth before its judges – Legal protection of minors in cyberspace’ (2011) 27 (1) CLSR 6, 10.

<sup>5</sup> UN General Assembly, *Convention on the Rights of the Child* (20 November 1989) UNTS vol 1577, 3, art 5 and art 12 / Srishti Virat, ‘Child Rights in the Digital Environment’ (2023) V (1) IJLLR 1 / John Tobin, *The UN Convention on the Rights of the Child: A Commentary* (OUP 2019).

<sup>6</sup> Reiner Schulze and Dirk Staudenmayer, *Digital Revolution: Challenges for Contract Law in Practice* (1st edn, Nomos 2016).

<sup>7</sup> Halla Holmarsdottir, Idunn Seland and Christer Hyggen, ‘How Can We Understand the Everyday Digital Lives of Children and Young People?’ in Halla Holmarsdottir, Idunn Seland, Christer Hyggen and Maria Roth (eds), *Understanding The Everyday Digital Lives of Children and Young People* (PM 2024).

<sup>8</sup> Francesco Rossi, *Capacità e incapacità* (ESI 2018).

protective model that assumes minors lack the maturity and awareness needed to undertake binding obligations. This approach finds parallels in German civil law jurisdiction, where §104 BGB provides that minors under the age of seven lack legal capacity entirely, and where contracts entered into by minors over seven are only valid with prior consent or subsequent approval by their legal representatives under §§107–109 BGB. This model, while conceptually aligned with the Italian system, enshrines a stricter mechanism of formal parental control.

As a general rule, minors are not entitled to validly conclude contracts except through their legal representatives or, where expressly provided, with judicial or parental authorisation<sup>9</sup>. However, this traditional model is increasingly challenged by the realities of digital interaction, in which minors regularly engage in activities that involve contractual relationships: accepting standard terms and conditions, making microtransactions, purchasing virtual goods, or subscribing to online services<sup>10</sup>.

Against this backdrop, one must question whether the codified approach to contractual capacity remains adequate to address the diffuse, low-value, and high-frequency contractual practices that characterise the digital economy<sup>11</sup>. The rigidity of the current legal regime may lead to dysfunctional outcomes, such as the systematic denial of contractual autonomy even in instances where the minor demonstrates sufficient understanding of the nature and consequences of the act. This calls for a reinterpretation of contractual capacity, not merely as a formal, age-based requirement, but rather as a functional competence to self-determine responsibly in specific contexts<sup>12</sup>.

---

<sup>9</sup> Guido Alpa, *Il contratto in generale. Principi e problema* (2nd edn, Giuffrè 2021).

<sup>10</sup> Fabio Bravo, 'I contratti a distanza e il mercato digitale' in Guido Alpa and Antonio Catricalà (eds), *Diritto dei consumatori* (IM 2016).

<sup>11</sup> Sandra Calvert, 'Children as Consumers: Advertising and Marketing' (2008) 18 (1) TFC 205.

<sup>12</sup> By analogy, the partition between *petits enfants* and *grands enfants*, relevant to health, self-determination and parental responsibility, would be applicable. See: Pasquale Stanzione, 'Persona minore di età e salute, diritto all'autodeterminazione, responsabilità genitoriale' (2013) CDC 21.

This perspective aligns with the CRC's principle of "evolving capacity", which calls for respecting minors' autonomy in proportion to their maturity<sup>13</sup>.

Private law reveals a tension between protectionist and enabling models, the former focused on vulnerability, the latter on graduated autonomy<sup>14</sup>.

A further dimension that requires analysis concerns the relationship between contractual capacity and the meritoriousness of interests pursued<sup>15</sup>. Pursuant to Article 1322 c.c., contractual autonomy may depend on whether the transaction serves a meritorious purpose<sup>16</sup>.

### **3. The Digital Contract: New Challenges**

The emergence of the digital contract marks a paradigmatic shift in the architecture of contractual relations<sup>17</sup>. Rather than serving as a negotiated exchange between parties of equal standing, the contract is increasingly embedded in digital infrastructures that automate consent, obfuscate content, and preclude authentic deliberation<sup>18</sup>.

Civil law has historically developed the architecture of contract on the basis of principles such as freedom of contract, equality between the parties, and the

---

<sup>13</sup> Sara Rigazio, 'A Dynamic Perspective on the Minor's Right to Self Determination: the Lesson from the Convention on the Rights of the Child (Crc) and Some Practical Insights from the Entertainment Industry' (2019) C.E.L.B. 3.

<sup>14</sup> Lucilla Gatt and Ilaria Amelia Caggiano, 'Consumers and Digital Environments as a Structural Vulnerability Relationship' (2022) 2 EJPLT 13 / Samuel Issacharoff, 'Disclosure, Agents, and Consumer Protection' (2011) 167 (1) JITE 65.

<sup>15</sup> Rosmawani Che Hashim and Farah Nini Dusuki, 'Minors and Their Incapacity to Contract: A Revisit' (2023) 14 (1) UUMJLS 269.

<sup>16</sup> Mariella Lamicela, 'La riscoperta del giudizio di meritevolezza ex art. 1322,co.2, c.c. tra squilibrio e irrazionalità dello scambio contrattuale' (2016) 5 (2) RG 195.

<sup>17</sup> Tatyana Skvortsova et al., 'Development of Digitization in Contractual Relations' (2019) 87 LNNS 1025.

<sup>18</sup> Nancy Kim, 'Digital Contracts' (2019) 75 TBL 1683.

significance of informed consent<sup>19</sup>. Yet, in the digital environment, these principles are often stripped of their substantive content. Consent is often expressed by clicking pre-ticked boxes, without individual negotiation<sup>20</sup>; general terms and conditions are unilaterally drafted, typically lengthy and technical, thereby rendering comprehension difficult even for the average adult user<sup>21</sup>; recommendation algorithms and personalised targeting mechanisms shape user choices, undermining the authenticity of contractual will<sup>22</sup>.

These criticalities become exponentially more pronounced when minors are involved. Their increased cognitive, emotional, and relational vulnerability exposes them to the risk of entering into binding obligations without a full awareness of the attendant legal and economic consequences<sup>23</sup>. In such cases, the digital contract risks degenerating into an instrument that constrains, rather than expresses, individual autonomy<sup>24</sup>. Private law must thus confront the adequacy of digital contracts in satisfying the requirements of conscious formation of consent, pre-contractual good faith, and equity in the performance of obligations<sup>25</sup>.

Moreover, the mass and serial nature of digital contracts introduces a structural tension between the individual dimension of contractual responsibility and the collective nature of digital market practices<sup>26</sup>. Online platforms do not operate on a relational basis but rather through automated and replicable models, in which

---

<sup>19</sup> Enrico Gabrielli, *I contratti in generale* (UTET 2006).

<sup>20</sup> Neil Richards and Woodrow Hartzog, 'The Pathologies of Digital Consent' (2018) 96 WULR 1461.

<sup>21</sup> Florian Mösllein, 'Digitized Terms: The Regulation of Standard Contract Terms in the Digital Age' (2023) 19 (4) ERCL 300.

<sup>22</sup> Mireia Artigot Golobardes, 'Algorithmic Personalisation of Consumer Transactions and the Limits of Contract Law' (2022) 1 JLMI 18.

<sup>23</sup> James Chang and Farnaz Alemi, 'Gaming the System: A Critique of Minors' Privilege to Disaffirm Online Contracts' (2012) 2 (2) UCILR 627, 642.

<sup>24</sup> Simona Tiribelli, 'Moral and Legal Autonomy in the Era of Artificial Intelligence' (2022) S&F 166.

<sup>25</sup> Martijn W Hesselink, *The Politics of the European Civil Code* (KLI 2006).

<sup>26</sup> Zeynep Ayata, 'European Union Contracts in Digital Environments' in David Ramiro Troitiño (ed) *E-Governance in the European Union* (Springer 2024) 173.

contractual content is unilaterally determined and the individual user has virtually no room for influence<sup>27</sup>.

This context calls into question the actual applicability of traditional civil law remedies—such as annulment for mistake or coercion, invalidity due to lack of form, or termination for breach—to scenarios that diverge markedly from the classical paradigm of deliberate and informed agreement.

Finally, the increasing integration of artificial intelligence into contractual processes—through chatbots, smart contracts, and dynamically personalised terms—raises novel questions concerning the legal attribution of will, the characterisation of offers, and the validity of consent expressed through automated interactions<sup>28</sup>. This debate must also be read in light of recent European legislation. The Digital Services Act<sup>29</sup> (Regulation EU 2022/2065) expressly prohibits certain manipulative practices—commonly referred to as ‘dark patterns’—and reinforces transparency duties, particularly where minors are concerned (art. 28). Similarly, the AI Act proposal prohibits systems that exploit the vulnerabilities of specific groups, such as children, by materially distorting their behaviour (art. 5). These measures show that the European legislator is moving towards a broader recognition of contractual vulnerability in digital contexts.

While these structural transformations raise concerns for all consumers, they become particularly problematic in the case of minors<sup>30</sup>. Here, the systemic opacity and automation of the digital contract intersect with specific legal and cognitive vulnerabilities, giving rise to compounded risks that private law must address with

---

<sup>27</sup> Antonio Orti Vallejo, ‘Contractual Relationships in Collaborative Economy Platforms’ (2019) 27 (5) ERPL 995.

<sup>28</sup> Norhafiza Awang, ‘Contract Law and Artificial Intelligence: Examine the Implications of AI on Contract Negotiation and Execution, Including the Challenges of Automated Contracting’ (2024) 7 IJARBSS 93.

<sup>29</sup> Regulation (EU) 2022/2065 of the European Parliament and of the Council on a Single Market for Digital Services (Digital Services Act) [2022] OJ L277/1. / Caroline Cauffman and Catalina Goanta, ‘A New Order: The Digital Services Act and Consumer Protection’ (2021) 12 (4) EJRR 758.

<sup>30</sup> Oleksandr Omelchuk, Olena Cherniak and Nataliia Tyshcuk, ‘Protection of the rights of children and minors in their transactions in the information society’ (2020) 9 (2) IH 25.

heightened sensitivity. It should be emphasised that vulnerability in digital contracting is not confined to minors. Situational vulnerabilities—such as impulsive behaviours induced by algorithmic recommendation systems or persuasive design techniques—may affect adult users as well. The European debate thus increasingly conceptualises vulnerability as a relative condition, not only linked to age, but also to the cognitive and relational context in which contractual decisions are made.

#### **4. The Minor in the Digital Contracts: Critical Issues**

Once minors enter this transformed contractual landscape, the criticalities described above become exponentially more severe. Their position as legally and cognitively unprepared subjects makes them particularly susceptible to contractual mechanisms that bypass understanding, inhibit negotiation, and impose obligations through design rather than dialogue<sup>31</sup>. The interaction between rules governing minors' legal capacity and the structural features of digital transactions necessitates a critical reassessment of the traditional mechanisms underpinning contractual obligation<sup>32</sup>.

First and foremost, digital contracts frequently lack any effective *ex ante* mechanism for verifying the user's legal status. This undermines the coherence of the protective legal framework, which is largely premised on the invalidity or voidability of acts entered into by those lacking capacity, while simultaneously exposing minors to obligations they may not fully understand or evaluate<sup>33</sup>.

The standardised nature of contractual terms on digital platforms further reduces minors' ability to comprehend and critically assess the content of contracts. This issue becomes even more acute in the presence of dark patterns or implicit persuasive

---

<sup>31</sup> Antonio Landi, 'I fornitori di servizi di intermediazione molto grandi' in Luca Bolognini, Enrico Pelino and Marco Sciadone (eds) *Digital Services Act e Digital Markets Act. Definizioni e prime applicazioni dei nuovi regolamenti europei* (TAL 2023).

<sup>32</sup> Irene Longo, 'Capacità e incapacità delle persone di età minore : alcuni spunti sul contratto telematico' (2016) 3 RIIG 391.

<sup>33</sup> Guido Alpa, 'I contratti del minore. Appunti di diritto comparato' (2004) 5 IC 517.

techniques, which may induce the minor to perform dispositive acts without an authentic manifestation of contractual intent<sup>34</sup>.

Another critical issue concerns the liability arising from contract performance. At the same time, the ability of legal representatives to invoke annulment under Article 1425 or appeal of the contract under Article 1426 of the Italian Civil Code may generate uncertainty in contractual relations, especially where the act in question has already produced significant economic effects or has been partially or fully executed<sup>35</sup>. Interestingly, German law adopts a more structured *ex-ante* approach: under §110 BGB (the so-called “Taschengeldparagraph”), minors may enter into contracts without parental consent only when the consideration is fully paid with means provided for that purpose. While this provision offers a narrow window of autonomy, it also implies a presumption of informed consent linked to financial limitation, which is absent in the Italian framework.

Additional concerns arise from evidentiary difficulties in proving minority status and lack of parental authorisation, particularly in digital environments that lack traceable or authenticated records<sup>36</sup>.

Finally, from an axiological perspective, a fundamental tension emerges between the principle of contractual freedom and the imperative of legal protection for minors<sup>37</sup>. On the one hand, minors are increasingly active participants in the digital economy, demonstrating growing relational and decision-making capabilities<sup>38</sup>; on the other

---

<sup>34</sup> Katri Nousiainen and Catalina Perdomo Ortega, ‘Dark Patterns in Law and Economics Framework’ (2024) 36 (1) LCLR 90.

<sup>35</sup> Francesco Rossi, ‘Contratti del minore e responsabilità per i danni prodotti alla controparte’ (2021) 1 Familia 3.

<sup>36</sup> If it is proved that the parents failed to exercise control and that the other party was harmed, the principle of *culpa in educando* may abstractly apply. See: Court of Cassation, Section 3, Civil, Judgment February 19, 2014 No. 3964.

<sup>37</sup> Eleonora Grossi, *La tutela del minore nel commercio elettronico e nella rete internet* (LIUC 2003).

<sup>38</sup> Anna Gambaro, ‘Il bambino consumatore: il suo diritto ad una appropriata informazione’ (2010) 12 SSF 221.

hand, there remains a pressing need for legal safeguards that cannot be wholly delegated to the logic of the free market<sup>39</sup>.

## 5. Protection and Empowerment

A first set of instruments comprises *ex ante* control mechanisms, aimed at preventing minors from entering into contractual relationships in conditions of unawareness or without supervision<sup>40</sup>. In this regard, the implementation of effective age verification systems represents a fundamental technical and legal requirement<sup>41</sup>. However, such systems must be carefully designed to strike a balance between legal certainty and the protection of minors' digital rights and privacy, avoiding disproportionate forms of profiling or surveillance<sup>42</sup>.

A further remedy lies in the adoption of enhanced contractual disclosures, drafted in simplified, comprehensible, and visually accessible language tailored to users in developmental stages<sup>43</sup>. In this sense, the imposition of a heightened duty of transparency upon digital service providers towards minor users is proposed, as a specific application of the general principle of pre-contractual good faith<sup>44</sup>.

---

<sup>39</sup> Novriyanto Nusi, 'Electronic Legality Of Employment Contracts On Minor Children' (2020) 2 (2) ESLAW 293.

<sup>40</sup> Shilpa Das, 'Ex-Ante Regulation: An Evolving Need in Digital Markets' (2024) 5 (1) CCIJOCLP 55.

<sup>41</sup> Simone Van Der Hof and Sanne Ouburg, 'We Take Your Word for It' - A Review of Methods of Age Verification and Parental Consent in Digital Services' (2022) 8 EDPLR 61.

<sup>42</sup> Karolina La Fors-Owczynik, 'Prevention strategies, vulnerable positions and risking the 'identity trap': digitalized risk assessments and their legal and socio-technical implications on children and migrants' (2016) 25 (2) ICTL 71.

<sup>43</sup> Natali Helberger et al., 'Digital Content Contracts for Consumers' (2013) 36 JCP 37.

<sup>44</sup> Virginia Portillo et al., 'A call to action: Designing a more transparent online world for children and young people' (2024) 19 JRT 1.

A third area of intervention concerns assisted validation or subsequent ratification mechanisms, whereby a contract entered into by a minor may acquire legal effect upon authorisation by a legal representative, potentially subject to judicial oversight<sup>45</sup>.

In Germany, a similar mechanism operates through §§108 and 109 BGB, which render the effectiveness of a contract concluded by a minor contingent upon the timely approval or rejection by their legal guardian. This institutionalised ratification system could inform future Italian reforms aiming to balance autonomy and protection in a predictable framework.

Particularly significant is the provision of a right of withdrawal without penalty<sup>46</sup>, exercisable within a reasonable period, as a post-contractual safeguard for acts undertaken without sufficient deliberation<sup>47</sup>. This remedy operates as an ex-post corrective, capable of neutralising detrimental effects without undermining the stability of legal transactions.

Lastly, it is essential to promote educational instruments grounded in private law. The dissemination of a culture of informed contracting, beginning at the school level, may constitute a structural measure of legal empowerment<sup>48</sup>. Digital contractual literacy should be understood not merely as a technical skill, but as the progressive exercise of individual autonomy, linked to the capacity to evaluate risks, consequences, and obligations. The inclusion of these safeguards finds further support in European legislation: while the DSA strengthens duties of transparency and limits on manipulative design towards minors, the AI Act<sup>49</sup> (EU Regulation n. 2024/1689) introduces a horizontal prohibition against exploiting users' vulnerabilities. Taken

---

<sup>45</sup> Jasper Verstappen, *Legal Agreements on Smart Contract Platforms in European Systems of Private Law* (LGTS 56, 2023) 55.

<sup>46</sup> Directive 2011/83/EU of the European Parliament and of the Council on consumer rights [2011] OJ L 304/64, art 9.

<sup>47</sup> Reinhard Steennot, 'The right of withdrawal under the Consumer Rights Directive as a tool to protect consumers concluding a distance contract' (2013) 29 (2) CLSR 105.

<sup>48</sup> Catherine M. Lemieux, 'Learning contracts in the classroom: Tools for empowerment and accountability' (2001) 20 (2) SWE 263.

<sup>49</sup> Regulation (EU) 2024/1689 (Artificial Intelligence Act) [2024] OJ L. / Celso Cancela-Outeda, 'The EU's AI act: A framework for collaborative governance' (2024) 27 IoT 2.

together, these provisions anticipate a model of digital private law in which contractual fairness is no longer measured exclusively by formal consent, but also by the substantive protection of vulnerable users.

## 6. Prospective Outlook: What Role for Private Law?

Yet, the centrality of contract as a mechanism for the voluntary regulation of legal relationships—especially in digital contexts—restores to private law a crucial role in constructing a legal order capable of reconciling liberty with protection. Regulating digital contracts demands an intelligent and selective adaptation of traditional legal institutions, without relinquishing the protective and axiological function of private law<sup>50</sup>.

In this light, private law must operate as a “second-generation” legal order, mediating between the individualistic logic of private autonomy and the imperative to protect vulnerable subjects, particularly minors<sup>51</sup>. The challenge, however, is not merely legal, but also institutional and cultural. A dialogical and intersystemic private law is needed—capable of engaging constructively with EU law (notably the AI Act, the DSA and the GDPR<sup>52</sup>), and with the pedagogical and constitutional dimensions of minor protection.

In this regard, private law cannot ignore the impact of the AI Act, which, alongside the DSA, shapes a European framework of digital fairness. Both instruments acknowledge that the manipulation of vulnerable individuals, whether minors or adults, constitutes a systemic threat to autonomy. These developments suggest a gradual convergence between consumer protection law, data regulation, and private law principles.

---

<sup>50</sup> Guido Alpa, ‘Il mercato unico digitale’ (2021) 1 CIE 1.

<sup>51</sup> Martha Albertson Fineman, *Equality, Autonomy, and the Vulnerable Subject in Law and Politics* (1st edn, Routledge 2013).

<sup>52</sup> Regulation (EU) 2016/679 (General Data Protection Regulation) [2016] OJ L119/1. / Felix Zopf, ‘Two Worlds Colliding - The GDPR in between Public and Private Law’ (2022) 8 EDPLR 210 / Ilaria Amelia Caggiano, ‘Protecting Minors as Technologically Vulnerable Persons through Data Protection: An Analysis on the Effectiveness of Law’ (2022) 1 EJPLT 27.

## 7. Towards a Digital Private Law for Childhood

The concept of contractual capacity, the principle of private autonomy, and the disciplines of information and liability must be reinterpreted in an adaptive manner—without abandoning doctrinal rigour but embracing a functional and dynamic reading<sup>53</sup>. In this respect, the proposal for a digital private law for childhood is not merely a theoretical aspiration; it is a systemic necessity. It calls for a legal space capable of articulating protection and empowerment, recognising the progressive maturation of the minor subject, and providing legal instruments that safeguard without excluding<sup>54</sup>.

The path forward is twofold: the elaboration of normative, jurisprudential, and doctrinal solutions that are consistent with the complexity of the digital environment; the promotion of basic legal education that enables minors to acquire awareness of their rights and obligations. From this perspective, private law is not merely a technical discipline, but a fundamental component of the democratic project, capable of contributing to a more just, transparent, and inclusive digital society. Looking ahead, the development of a digital private law framework for minors may contribute to building a more just, inclusive, and proportionate legal system—one in which minors' participation in economic life is not relegated to a regulatory grey area, but governed by principles of shared responsibility, graduated autonomy, and effective protection<sup>55</sup>.

---

<sup>53</sup> Mark Tunick, 'State Authority, Parental Authority, and the Rights of Mature Minors' (2023) 27 TJE 7 / Grzegorz J. Blicharz, 'Consumers as Unassisted Minors: Asymmetrical Sanction for Unfair Contract Terms' (2022) 11 (6) Laws 87.

<sup>54</sup> Liat Franco and Shulamit Almog, 'Precarious Childhood: Law and its (IR)Relevance in the Digital Lives of Children' (2019) 7 (1) PSJLIA 53.

<sup>55</sup> Charles Alves de Castro, Aiden Carthy and Isobel O'Reilly Dr, 'An Ethical Discussion About the Responsibility for Protection of Minors in the Digital Environment: A State-of-the-art review' (2022) 9 (5) ASSRJ 343.



## LET'S PLAY TOGETHER: FAIR RULES FOR MINOR VIDEO GAMERS A RESEARCH AGENDA

Federica Casarosa\* and Lavinia Vizzoni\*

### Abstract

This short paper provides for a research agenda dedicated to the critical position of minors as video game players in the EU scenario. Firstly, minors are contextualized in the digital scenario as primary users of several applications, also AI-based, but at the same time exposed to the consequent risks. Then, the specific case of young video gamers is considered, with its implications related to crucial issues like the processing of minors' personal data, unfair business practices and the nature of the video game itself.

In the EU legal framework, few solutions emerge, however, along with some confusion and overlapping rules. The contribution aims at highlighting such challenges, providing initial indications to be further discussed in academic literature on how to protect minor gamers, with the objective of finding effective solutions without, at the same time, excluding children from entertainment.

### Table of contents

LET'S PLAY TOGETHER: FAIR RULES FOR MINOR VIDEO GAMERS A RESEARCH AGENDA .....	217
Abstract.....	217
Keywords.....	218
1. Introduction. Minors in the digital context between risks and opportunities	218

---

\* Federica Casarosa is a Research Affiliate at the Scuola Superiore Sant'Anna and Lavinia Vizzoni is a Tenure-track Assistant Professor at the University of Pisa. Double blind peer reviewed contribution.

2. An underestimated risk: the use of video games by minors.....	222
3. Buying and downloading options for video games .....	225
4. AI-based systems embedded in video games .....	228
5. Communication tools and platform regulation.....	230
6. Tentative conclusions .....	232

## Keywords

Minors – Video games – Data protection – Artificial intelligence – Capacity of discernment

### **1. Introduction. Minors in the digital context between risks and opportunities**

The rapid development and consequent massive diffusion of scientific and technical knowledge and applications<sup>1</sup> has affected all areas of individuals' activities, and specifically, it has prompted a profound debate concerning the role and protection of the person under the age of 18 years. Among the different perspectives, an interesting dimension emerges, giving rise to a new chapter in the regulation of juvenile and family law:<sup>2</sup> Gaming and virtual reality played by minors.<sup>3</sup>

In general, minors commonly make use of applications that employ digital technologies, sometimes supervised and/or supported by their parents and relatives, sometimes, instead, in complete autonomy.<sup>4</sup> Statistics show that minors are the users

---

<sup>1</sup> On the relationship between law and science, see Giorgio Oppo, 'Scienza, diritto, vita umana', in Riv. dir. civ. (2002) I, 11 who points out that applied science, and thus technology, is ontologically destined to be regulated by law. See also, Guido Alpa, 'Tecnologie e diritto privato, in Riv. it. sc. giur. (2017) 205.

<sup>2</sup> Talks about new "dimension" of family law Amalia Chiara Di Landro, 'Best interest of the child e tutela dei minori nel dialogo tra legislazione e giurisprudenza, giurisprudenza' in Nuove leggi civ. comm. (2020) 2, 452. On the relationship between new technologies and family law and the theorization of a kind of "cyberfamily," see Sandro Nardi, *La famiglia e gli affetti nell'era digitale*, Naples, 2020, 7 ff. and with specific regard to children, 39 ff.

<sup>3</sup> M. V. Birk, S. van der Hof, and A. van Rooij, 'Behavioral design in video games' in Games: Research And Practice (2024) 2(2), 1-3; E. Fosch Villaronga, et al., 'Toy story or children story?: Putting children and their rights at the forefront of the artificial intelligence revolution' in Ai & Society (2021) 38(1), 133-152.

<sup>4</sup> Francesco Di Ciommo, *Evoluzione tecnologica e regole di responsabilità civile* (ESI, 2003) 32 ff. On the massive diffusion of new technologies in the daily lives of minors as well, see also Emanuela Andreola, *Minori e incapaci in Internet* (ESI, 2019) 22 ff.

par excellence of certain content:<sup>5</sup> from accessing and surfing the Net, to browsing social networks, usually through smartphones. These activities exploit devices whose operation maybe also based on Artificial Intelligence systems, interconnected within Internet of Things,<sup>6</sup> such as wearables,<sup>7</sup> smart home speakers<sup>8</sup> or smart toys, as well as video games consoles. However, such high diffusion is not always coupled with knowledge and awareness of the risks emerging from such an environment.<sup>9</sup> An example of the possible risks comes from the affair of the “Hello Barbie” smart toy: the Mattel doll released in 2015 was equipped with a microphone and software able to interact with children. However, the conversations were not just a trigger for the reactions of the doll but were recorded and stored on cloud, after the interaction. Then, the recordings were transmitted to a California company specialized in the development of AI systems, with the aim of improving the relevance and quality of the interaction the toy has with its young owner.<sup>10</sup> When this process was uncovered, issues regarding data protection and security were raised along with claims regarding bias and discrimination in the speech interactions provided, leading to the discontinuation of the smart toy production.

The example shows that minors, more candid and willing to engage in imaginative play, are less conscious of the risks, and may become victims of offences perpetrated through smart technologies.<sup>11</sup> Thus, the potential fragility of minors demands special

---

<sup>5</sup> Unicef, The State of the Children in the European Union in 2024. In particular, the statistics show that in 2023 in the EU, 97 % of people under 15 have access to Internet”. See the Digital technology policy brief at <https://www.unicef.org/eu/media/2826/file/Digital%20technologies%20policy%20brief.pdf.pdf>.

<sup>6</sup> See Rolf H. Weber, ‘Internet of Things - Need for a New Legal Environment?’, in Computer Law & Security Review (2009) 521. On the potential of the IoT, see Amedeo Santosuosso, *Intelligenza artificiale e diritto* (Giuffrè, 2020) 180 ff.

<sup>7</sup> See Italian Data Protection Authority Order No. 179 of March 26, 2015, Launching the Public Consultation on the Internet of Things.

<sup>8</sup> Lavinia Vizzoni, *Domotica e diritto. La Smart Home tra regole e responsabilità* (Giuffrè, 2021) 72 ff.

<sup>9</sup> For an overview of the digital risks see UNICEF (n. 5), p. 4. See also Ronny Bogani and Burkhard Schafer, ‘Artificial Intelligence and Children’s Rights’, in Marcello Ienca et al. (eds), *The Cambridge Handbook of Information Technology, Life Sciences and Human Rights* (Cambridge University press, 2022), 217 ff.

<sup>10</sup> On the matter, see Irina D. Manta, David S. Olson, ‘Hello Barbie: First They Will Monitor You, Then They Will Discriminate Against You. Perfectly’ 67 *Alabama Law Review* (2015)135.

<sup>11</sup> See also Bogani and Schafer (n. 9) who underline that children are more vulnerable than adults due to their developmental psychology and in particular to “*their emotional volatility and impulsiveness, which provides a unique opportunity for online marketers to reach a particularly vulnerable target customer market*”, 218.

attention.<sup>12</sup> Indeed, the consequences of uncontrolled exposure to the risks of the digital ecosystem can become devastating with respect to subjects who, being physiologically in a psycho-physical condition of vulnerability, it is easily influenced in their capacity for self-determination.<sup>13</sup>

However, the aforementioned risks must not outweigh the benefits springing from the use of technologies. The use of various digital tools by minors represents a form of manifestation of their personal and digital identity, integrating a decisive moment in the formation of their personality, in a context in which the physical world and the virtual world represent two articulations of the same space of relationship.<sup>14</sup> This is confirmed by fundamental rights principles and declarations both at the supranational and at the national levels: first, the UN Convention on the Rights of the Child (hereafter UN CRC)<sup>15</sup> recognizes that the welfare and development of children should be protected, allocating a set of rights to children; then, Art. 24 of the EU Charter of Fundamental Rights affirms that children's well-being entails protection and care, as well as recognition of their opinions and choices.<sup>16</sup> In more general terms, finally, Article 2 of the Italian Constitution implies that the minor can freely express and develop his or her personality, which means that the minor can freely move in that direction for the realisation of their identity interests.<sup>17</sup>

---

<sup>12</sup> The delicate relationship between young users and the Internet is investigated, among others, by Alessandro Mantelero, 'Teens online and data protection in Europe' in *Contr. impr. Europa* (2014) 442., Id, 'Children online and the future EU data protection framework: empirical evidences and legal analysis' in *Int. J. Technology Policy and Law* (2016) 169, Carolina Perlingieri, 'La tutela dei minori di età nei social networks' in *Rass. dir. civ.* (2016) 1324.

<sup>13</sup> Talks about the "vulnerability" of the "electronic body" of "digital native minors", Antonina Astone, *I dati personali dei minori in rete. Dall'internet delle persone all'internet delle cose* (Giuffrè, 2019) 5 ff; Ilaria Garaci, 'Il "superiore interesse del minore" nel quadro di uno sviluppo sostenibile dell'ambiente digitale' in *Nuova giur. civ. comm.* (2021) 801.

<sup>14</sup> See Arianna Thiene, 'I diritti della personalità dei minori nello spazio virtuale', in *Annali online did. e form. doc.* (2017) 13/2017, 26.

<sup>15</sup> Convention on the Rights of the Child, adopted on 20 November 1989, by General Assembly resolution 44/25.

<sup>16</sup> M. Kellerbauer, M. Klamert, and J. Tomkin (eds), 'Article 24 CFR', in Manuel Kellerbauer, Marcus Klamert, and Jonathan Tomkin (eds), *The EU Treaties and Charter of Fundamental Rights: A Commentary*, 2nd Edition (Oxford Law Pro, 2024) 520.

<sup>17</sup> Roberto Senigaglia, *Minore età e contratto. Contributo alla teoria della capacità* (Giappichelli, 2020), 75; Id, 'L'identità personale del minore di età nel cyberspazio tra autodeterminazione e parental control system', in *Nuove leggi civ. comm.* (2024) 6, 1568. And formerly, see Francesco D. Busnelli, 'Immagini vecchi e nuove della tutela della salute del minore', in Andrea Bucelli (ed.), *Identità e salute del minore* (Pisa University Press, 2021) 3. More recently,

Within this context, this contribution aims to provide a research agenda that considers two main challenges emerging from the policy perspective and from the academic perspective. On the one hand, the contribution aims at identifying the risks and problems that result from the restrictive approach adopted in some countries as regards the use of technology by minors: imposing a ban, or strict limitation, for minors in general, such as, for instance, in the Italian draft bill on Protection of minors in the digital environment,<sup>18</sup> is in clear contrast with the evolving capacity of discernment that minors acquire throughout the years. Such development is acknowledged by international treaties, such as the abovementioned UN CRC. How has the evolving capacity of discernment of minors been taken into consideration by the legislator so far? Is there a difference between the approach adopted at the European and national levels? Which are the criteria that the legislator has identified to show the development in the capacity of discernment?

On the other hand, the analysis of the academic literature on the protection of minors has so far approached this topic from a sectoral perspective, for instance, looking specifically at the specific rules applicable to protect minors' personal data,<sup>19</sup> or discussing the risks of cyberbullying,<sup>20</sup> etc. Few are the occasions in which the analysis is full-fledged and encompasses the overall activity of the minor in the digital realm.<sup>21</sup>

---

Daniela Marcello, *Circolazione dei dati del minore tra autonomia e controllo. Norme e prassi nel mercato digitale europeo* (ESI, 2023) 51.

<sup>18</sup> The draft bill in question was presented to the Chamber of Deputies and the Senate on 13 May 2024 and is currently under examination in committee. On its main contents and critical issues see Lavinia Vizzoni, *I "minori digitali" tra doveri educativi e tutele* (Bari, 95 ff.)

<sup>19</sup> With specific regard to the processing of a child's personal data, see Antonina Astone, *I dati personali dei minori in rete. Dall'Internet delle cose all'Internet delle persone* (Milano, 2019) *passim*, Daniela Marcello, *Circolazione dei dati del minore tra autonomia e controllo. Norme e prassi nel mercato digitale europeo* (Napoli, 2023) *passim*. See also I. A. Caggiano, 'Protecting Minors as Technologically Vulnerable Persons Through Data Protection: An Analysis on the Effectiveness of Law' (2022) *European Journal of Privacy Law & Technologies*.

<sup>20</sup> On the phenomenon of cyberbullying and strategies for its counteraction, see Carolina Perlingieri, *Profilo civilistico dei social networks* (Napoli, 2014) 33 ff., Anna Carla Nazzaro, 'Cyberbulismo' in *Tecnol. e dir.*, 2020, n° 2, 465 ff., Ettore Battelli, 'Minori e social network: cyberbulismo e limiti della parental responsibility' in *Corr. giur.*, 2021, n° 10, 1269 ff., Francesca Zanovello, 'Prevenzione e contrasto del bullismo e del cyberbulismo. Tra novità e criticità della l. n. 70/24' in *Nuove leggi comm.*, 2024, n° 4, 826 ff. For an analysis of cyberbullying and online abuse from a criminological and legal perspective, proposing strategies to improve the digital environment see also F. Ahmed, F. Chaudhary, & S. Shahzad, *Cyberbullying and Online Harassment: A Criminological and Legal Perspective*. *Policy Research Journal*, (2025) 3(2) *Policy Research Journal* 52–59.

<sup>21</sup> See the attempt to outline a comprehensive legal framework for the digital minors by Vizzoni (n. 18) at 57 ff., and with specific regard to the position of parents, at 121 ff.

The present contribution will instead adopt a different methodology in order to identify the several legal dimensions that the use of technology may trigger. This will allow not only to have a clear picture of the emerging risks that the minor will face, but also identify if and how the legislative interventions may coordinate and provide for synergies in order to solve or mitigate the risks, or vice versa may overlap and contradict potentially imposing additional burdens to manufacturers of ICT that, indirectly, impact on the abilities of minors to fully exercise their rights.

According to the above-mentioned objectives, the role of minors in the digital environment will be investigated, focusing on the use of (online) video games. This will allow us to highlight the importance of such increasingly sophisticated applications and devices for the lives of minors, as well as the related risks, especially when AI-based tools and services are embedded. Special attention will be devoted to the balance between the legislative framework, still anchored to an age-based definition of minors, vis-à-vis the expanding autonomy of minors in the practices, able to show evolving capabilities. Special attention will be paid to the Italian legal system implementing and integrating with the EU legislation.

The results of this initial exploration, which will consider some practical cases too, will then provide some tentative interim conclusions in order to delineate a conceptual foundation for further scholarly inquiry and legislative consideration.

## **2. An underestimated risk: the use of video games by minors**

Video games are a daily feature in minors' lives.<sup>22</sup> Many options are available for individual play, that engage the minor in a solitary challenge that can either require an Internet connection or not, but also multiplayer games, where the added value is provided by the possibility to play online with other users, which may or may not be known by the minor. Additionally, virtual reality games are also available, where simulated experiences require additional devices in order to enhance immersion in virtual reality.

---

<sup>22</sup> J. Gottfried and O. Sidoti, *Teens and Video Games Today* (Pew Research Centre, 2024), available at <https://www.pewresearch.org/internet/2024/05/09/teens-and-video-games-today/>

The use of video games by minors is not only a means of entertainment, but also, depending on the type of interaction and features available, video games become a tool to engage with friends, connect with people with the same interests, experiment with personal identity, and enhance imagination.<sup>23</sup> The positive effects of video games do not exclude the risks that emerge from prolonged and assiduous use, affecting the ability to restrain and engage in social interactions,<sup>24</sup> or the risks of exposure to harmful or unlawful content.<sup>25</sup>

Such risks may be enhanced by the design choices of video game manufacturers. If, in the early days of video games, the business models adopted by manufacturers were based on direct micro-payments, through the availability of consoles in arcades, or on the purchase of the entire games on a physical support that allowed the gamers to play at home, nowadays manufacturers have widened their business models through advertisement and/or user-data driven models.<sup>26</sup> As a matter of fact, in order to generate profit, video games are designed in a way to enhance the participation and engagement; although, in principle, this is legitimate from the manufacturer's perspective, it becomes problematic as soon as the design choices lead to economic

---

<sup>23</sup> The importance of play in the development of minors is also recognised by the UN Committee on the Rights of the Child, 'General comment No. 14 2013 on the right of the child to have his or her best interests taken as a primary consideration (art. 3, para. 1)' (2013), available at: [https://www2.ohchr.org/English/bodies/crc/docs/GC/CRC\\_C\\_GC\\_14\\_ENG.pdf](https://www2.ohchr.org/English/bodies/crc/docs/GC/CRC_C_GC_14_ENG.pdf). The document affirms that "Play and recreation are essential to the health and well-being of children and promote the development of creativity, imagination, self-confidence, self-efficacy, as well as physical, social, cognitive and emotional strength and skills. They contribute to all aspects of learning: they are a form of participation in everyday life and are of intrinsic value to the child, purely in terms of the enjoyment and pleasure they afford. [...] Play and recreation facilitate children's capacities to negotiate, regain emotional balance, resolve conflicts and make decisions." (at p. 4). See also Simone van der Hof et al., "Don't Gamble With Children's Rights"—How Behavioral Design Impacts the Right of Children to a Playful and Healthy Game Environment' *Front. Digit. Health* (2022) 4:822933, 5, where several examples of healthy games are presented.

<sup>24</sup> The psycho-social literature has long highlighted the substantial risks inherent in the use of video games by infants and adolescents, which may also result in addiction. Cfr. P. Ghezzo and G. M. Pirone, 'Videogiochi e minori, le questioni aperte', in *Difesa sociale* (2007) 1, 11; F. Romano and M. Conti, 'La dipendenza da videogiochi', in *Psicologia di comunità* (2014) 1, 71. More in general, on the anxiety that affects Gen-Z people, see Jonathan Haidt, *The Anxious Generation: How the Great Rewiring of Childhood Is Causing an Epidemic of Mental Illness* (Penguin Books Ltd, 2025) 20 ff. The author identifies two trends: overprotection in the real world and underprotection in the virtual world as the major reasons why children born after 1995 became the so-called anxious generation.

<sup>25</sup> See Van der Hof et al (n. 23) who distinguish among different types of harm: social harm (e.g., invasion of privacy, hate speech or cyberbullying), mental harm (e.g., sexual abuse or aggression from playing violent games), physical harm (lack of exercise, obesity, poor sleep), at 6.

<sup>26</sup> See Max V. Birk, Simone van der Hof, and Antonius J. van Rooij 'Behavioral Design in Video Games', *ACM Games* 2, 2, Article 16 (August 2024).

exploitation of gamers, and in particular minors. Such an exploitation can emerge through different forms: unlawful personal data processing,<sup>27</sup> manipulation of economic choices, and a push towards harmful activities.<sup>28</sup>

These are not only theoretical risks, as a recent U.S. case has uncovered a real “Pandora’s box”. In 2022, Epic Games, the company that owns the famous video game Fortnite, was the recipient of a substantial fine following a settlement with the Federal Trade Commission.<sup>29</sup> The challenged conduct pertained to the collection of personal data of users under the age of thirteen<sup>30</sup> - such as their names, email addresses, identifiers used to track players’ progress, purchases made, game settings, and friends lists – without the consent neither of the minor, nor of the parent. The investigation uncover that such activity was malicious as the company’s data controller was perfectly aware of the data collection.

Additionally, the Federal Trade Commission imposed a sanction for the manipulation of minors put in place by Epic Games: the company in order to push underage users to purchase virtual goods used dark patterns, essentially carrying out unfair business practices, inducing underage players to make purchases that could take place without parental consent.<sup>31</sup>

Although the case was solved based on the U.S. legal framework, it highlights a set of problems that may also be translated into the European context. Which are the legal provisions that may be applicable to video games? The following sections will try to identify an initial overview of the problems taking the perspective of the minor user. Given that different (and overlapping) pieces of legislation apply, the following

---

<sup>27</sup> Not only is the creation of children profiles, without their (or their parents’) consent is unlawful but it may also be exploited directly and indirectly: for instance, the video game manufacturer can send reminders to the email account of the player to rejoin the game; or can share or sell the personal data to third parties.

<sup>28</sup> Van der Hof at al. (n. 23) at 7.

<sup>29</sup> See Fulvio Sarzana di S. Ippolito, ‘Fortnite viola la privacy di minori e li inganna: così la super sanzione da 520 milioni di dollari’, in *cybersecurity360.it*, 20 dicembre 2022

<sup>30</sup> The thirteen-year limit arises from the U.S. *Children’s Online Privacy Protection Act* (COPPA) of 1998. See Sasha Grandison, ‘The Child Online Privacy Protection Act: The Relationship Between Constitutional Rights and The Protection of Children’, in *University of the District of Columbia Law Review* (2011) 14(1) 209.

<sup>31</sup> See Tommaso Crepax and Jan Tobias Muehlberg, ‘Upgrading the Protection of Children from Manipulative and Addictive Strategies in Online Games: Legal and Technical Solutions Beyond Privacy Regulation’, in *International Review of Information Ethics*, 31(1), 1 ff. (2022): the authors analyse manipulative and addictive strategies in online games for children and proposes legal and technical solutions to enhance their protection.

analysis will look upon the practical steps that the minor will follow when deciding to engage with video games: from the moment of the purchase or download of the video game, where national contractual rules apply; to the moment of play, where the recent European legislation on Digital Services Act and AI act apply, as well as the provisions on unfair commercial practices; and the possibility to communicate and engage with other players, triggering the application of the General Data Protection Regulation.

### **3. Buying and downloading options for video games**

Although minors are the users par excellence of video games, their act of purchase or download of such video games raises some doubts about the validity of the relevant contract of sale/supply. In the Italian legal system, minors are considered to be structurally fragile, vulnerable people, who raise protective needs, which are centred essentially on the dogma of the minor's absolute incapacity to act, pursuant Article 2 of the Italian Civil Code. But of course, a static solution, where the minor, regardless of their age and effective capacity, is prevented from carrying out any legally relevant act, does not grasp the complexity of the present and the variety of dynamics in which the underage person is the leading actor.

Therefore, there are several instances that enhance the autonomy of the minor. Still, in the Italian civil code, there are so called "exceptions" to the incapacity rule. For example, under some conditions and over a certain age, a minor can work and recognise a child born out of wedlock. And the emancipated minor has a partial capacity. The real change is due to the already mentioned international charters of rights, especially the UN CRC, which adopted for the first time at the international level the well-known principle of the best interest of the child.<sup>32</sup> This principle, which has to drive every decision in which an underage person is involved, and the two other

---

<sup>32</sup> See Arianna Thiene, 'I diritti della personalità dei minori nello spazio virtuale', in *Annali online did. e form. doc.* (2017) 13/2017, 26.

<sup>32</sup> On the best interest of the child see, among others, Enrico Quadri, 'L'interesse del minore nel sistema della legge civile', in *Famiglia e dir.* (1999) 80, Leonardo Lenti, 'Best interests of the child' o «best interests of children»?, in *Nuova giur. comm.* (2010) 157, Vincenzo Scalisi, 'Il superiore interesse del minore, ovvero il fatto come diritto', in *Rivista di diritto civile* (2018) 405, Michele Sesta, 'La prospettiva paidocentrica quale fil rouge dell'attuale disciplina giuridica della famiglia', in *Famiglia e dir.* (2021), 763 ff., Elisabetta Lamarque, 'Pesare le parole. Il principio dei best interests of the child come principio del miglior interesse del minore', in *Famiglia e dir.* (2023), 365 ff.

principles that derive from it, that is to say, the right of the minor to be heard,<sup>33</sup> and the capacity to discern,<sup>34</sup> build the new value triad of juvenile law.

The capacity to discern is presumed to have been acquired at the age of twelve, although its existence can be proved even before. The evaluation of discernment is an assessment of the single minor and requires a careful, concrete investigation, a specific analysis to be carried out case-by-case in order to prove the real maturity of the individual.<sup>35</sup> The reference to an age threshold other than the eighteenth year, which has always traditionally worked as a border between incapacity and capacity to act, is particularly meaningful. Another “dogma” seems this way to be shattered, the undifferentiated category of the minor, inclusive of individuals from zero to eighteen years,<sup>36</sup> expressive of what has been called a «uniform and flattened view of reality».<sup>37</sup> And yet, the doctrine's reflection has gone further. As already said on the side of personal acts, a wide area of autonomy has long been recognized for the minor. Some openings are now shown even toward a contractual capacity of the minor, recognizing the minor capable of discernment, the ability to perform even those acts that, although expression of the exercise of patrimonial rights, are functional to the implementation of personal rights, in accordance with the constitutional right to pursue the development of their personality.

---

<sup>33</sup> On the minors' right to be heard, see Cesare Massimo Bianca, 'Il diritto del minore all'ascolto', in *Nuove leggi civ. comm.*, 2013, 546 ff., Pietro Virgadamo, 'L'ascolto del minore in famiglia e nelle procedure che lo riguardano', in *Dir. fam. pers.* (2014) 1656 ff.

<sup>34</sup> See, also from a critical perspective, Giovanni De Cristofaro, 'Il diritto del minore capace di discernimento di esprimere le sue opinioni e il c.d. ascolto fra c.p.c. riformato, convenzioni internazionali e diritto UE', in *Familia*, (2023), 363.

<sup>35</sup> On the different capacities and abilities of minors, see Grace Icenogle et al. 'Adolescents' cognitive capacity reaches adult levels prior to their psychosocial maturity: Evidence for a "maturity gap" in a multinational, cross-sectional sample', in *Law and human behavior* (2019) 73. In particular, the authors distinguish between "cold" cognition and "hot" cognition, the former refers to "mental processes (such as working memory or response inhibition) employed in situations calling for deliberation in the absence of high levels of emotion", where young adults perform comparably to older individuals; while the latter "involves mental processes in affectively charged situations where deliberation is unlikely or difficult", where instead the young adults show striking differences with older individuals.

<sup>36</sup> Francesco Donato Busnelli, 'Capacità ed incapacità di agire del minore', in *Persona e famiglia. Scritti di Francesco D. Busnelli*, Pisa, (Giappichelli, 2017), 216.

<sup>37</sup> The suggestive words are from Pietro Rescigno, 'Una ricerca sui minori', in Marcello De Cristofaro, Belvedere (eds) *L'autonomia dei minori tra famiglia e società*, (Giuffrè 1980), XI.

The General Data Protection Regulation (GDPR)<sup>38</sup> highly contributed to consolidating a new role for minors. According to the GDPR framework, minors require special protection regarding the processing of their personal data, as they may not be fully aware of the risks, consequences, and security measures related to such processing. In particular, Article 8 establishes that the processing of minors' personal data is lawful only if the minor is at least sixteen years old; otherwise, parental or guardian consent is required. Member states can lower this threshold, not under thirteen years, as Italy has done, setting the age at fourteen.<sup>39</sup>

So, minors who are at least fourteen years old can provide their consent personally for the processing of data, in relation to information society services, such as registering on social networks. This recognition of the capacity to give consent is closely linked to the possibility of recognizing the minor's capacity to enter into contracts, related to the provision of such services.

In the video games field, it has to be highlighted, though, that first of all, there is no control, so the purchase of the video game is limited to those indicated as suitable for the age group to which the young user belongs.<sup>40</sup> Sometimes, in fact, users are anything but great minors capable of self-determination and of making autonomous and wise choices in function of the development of their personality, assuming that such a function can be configured regarding the purchase of such a product/service.

As regards giving consent to the processing of the user's personal data in the context of an information society service, often the minor data subject is well below the age limit of fourteen, relevant in the Italian legal system, as well as in other EU legal systems, to provide a valid, autonomous consent. Besides, the capacity to give personal consent is not necessarily symmetrical to the capacity to enter into the

---

<sup>38</sup> Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.

<sup>39</sup> See C. Caglar, 'Children's Right to Privacy and Data Protection: Does the Article on Conditions Applicable to Child's Consent Under the GDPR Tackle the Challenges of the Digital Era or Create Further Confusion?' (2022) *European Journal of Privacy Law & Technologies*, where the author examines whether the provision on the conditions applicable to a child's consent under the GDPR addresses the challenges of the digital age or merely adds complexity, L Jialin, 'Reflection on Data Right Protection for Minors in the Digital Age' (2025) *Children and Youth Services Review*, in which the author proposes an expansion of the protection of minors' sensitive information, emphasising the responsibilities of data controllers.

<sup>40</sup> Giovanni Ziccardi, 'I minori online tra videogiochi e metaverso, in Ciberspazio e dir. (2023) 3, 325.

connected contract. The main underlying issue is whether the contract of purchase/download of a video game can be considered as functional to the development of the minor's personality, in the digital environment. This specific answer actually depends greatly on the age of the minor and on the circumstances of the case.

Even if the underage user is above the fourteen years threshold, and the related contract is considered to contribute to the development of the minor, there are still several matters to solve: regarding the category of "older" users, first of all there is the need not to exclude them from entertainment, but also to correctly identify the applicable rules, in order to protect them properly, in a multi-level perspective.

#### **4. AI-based systems embedded in video games**

The "digital issues" arising from the use of AI-based technologies, also with regard to minors, have recently been addressed by the so-called Artificial Intelligence Act,<sup>41</sup> having the objective of improving the functioning of the internal market and promoting the adoption of reliable and human-centred Artificial Intelligence, while ensuring a high level of protection of the fundamental rights enshrined in the Charter of Fundamental Rights.

The Regulation, adopting a risk base approach that now dominates the regulation of new technologies, is strongly focused on the categorisation of AI systems according to the risk they generate<sup>42</sup>. This ranges from unacceptable risk, which makes the use of the AI systems prohibited, to high risk, so that the AI systems defined as such are required to meet stringent requirements under the Regulations, including risk mitigation measures, to minimal risk, which does not require the fulfillment of any

---

<sup>41</sup> Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act).

<sup>42</sup> Giusella Finocchiaro, 'La regolazione dell'intelligenza artificiale', in Riv. trim dir. pubbl. (2022) 4, 1085, part. 1093 ff.

obligations under the AI Act,<sup>43</sup> but providers are encouraged to voluntarily adopt additional codes of conduct.

There is also a limited, “specific transparency” risk: as clarified by the European Commission itself in a statement, the official communiqué of August 1<sup>st</sup> 2024, on the entry into force of the AI Act,<sup>44</sup> systems that fall under it, such as chatbots, must clearly inform users that they are interacting with a machine, while some content generated by AI must be explicitly labelled as such.

The category of the minimum risk of AI-based systems, when compared to their use by minors, arouses immediate perplexity, especially when the Commission, in its communiqué, refers to AI systems characterised by a minimum risk, by way of example, “video games that exploit AI”. The risks of such a qualification may enhance the possibilities of exploitation against minors, as video games already exploit several algorithmic or AI-based tools. The (slightly) less worrisome ones relate to, for instance, the use of dynamic difficult adjustments,<sup>45</sup> which allow the possibility to reduce the difficulty of the game every time the player fails to reach the conclusion of the game. Although this technical adjustment aims at keeping the player interested in the game from the beginning to the end, it may also affect the player's ability to disengage, resulting in an infinite game duration. Other cases instead are more problematic, as for instance, the case of monetized matchmaking which is based on the possibility of linking players (with different levels of expertise) in such a way as to trigger the less expert player to purchase items or goods (internal to the game) used by the more expert one. It is clear that in this case, the AI-based system allocates the linked players based on players' data, including not only game-based data (such as skill level items used, amount of time dedicated to the game, etc.) but also personal data. Clearly, this type of application results in encouraging microtransactions rather than increasing the actual quality or playability of the game.<sup>46</sup>

---

<sup>43</sup> Note that apart from the general obligation regarding AI literacy envisaged in Art. 4, no additional requirements in the design, development and deployment of the AI system are applicable.

<sup>44</sup> See [https://commission.europa.eu/news/ai-act-enters-force-2024-08-01\\_it#:~:text=Il%201%C2%BA%20agosto%202024%20%C3%A8,intelligenza%20artificiale%20nell'UE.](https://commission.europa.eu/news/ai-act-enters-force-2024-08-01_it#:~:text=Il%201%C2%BA%20agosto%202024%20%C3%A8,intelligenza%20artificiale%20nell'UE.)

<sup>45</sup> See more at [https://en.wikipedia.org/wiki/Dynamic\\_game\\_difficulty\\_balancing](https://en.wikipedia.org/wiki/Dynamic_game_difficulty_balancing).

<sup>46</sup> Van Der Lot et al. (n. 23) at 10.

## 5. Communication tools and platform regulation

Coming specifically to the potentially underestimated risks that the use of video games can produce on underage users, firstly, it is rare that video games do not avail themselves of solutions declined in terms of chatbots: the configuration of a “customer service” answering FAQs is sufficient for this purpose; and furthermore, in narrative video games, it is precisely a chatbot that appears by default, perhaps with human features, to answer the player’s questions.

So, in this way, the video game *tout court* has already trespassed into the category of limited risk of the AI Act mentioned above, which nevertheless requires the fulfilment of mere transparency obligations, so that, as mentioned, the user is informed that he or she is interacting with a machine.

Along with chatbots, another feature available on video games is the possibility of interacting with other players through messaging systems or directly with conversations that take place through headsets equipped with a microphone. This feature is not without issues too: a first question emerging is the classification of the messaging service according to the legal framework. This qualification depends upon the level of integration within the game itself, in some cases it is fully integrated (and therefore operated by the same manufacturer of the video game), in other cases it may be provided by third party service providers, as exemplified by widely used platforms Discord.<sup>47</sup> This element is not without relevance, as the classification of the service may, in turn, bear on the legal nature of the video game itself. Indeed, one might contend that enabling interpersonal communication among players effectively transforms the video game into a digital platform, thereby rendering it subject to the regulatory obligations imposed by the Digital Services Act<sup>48</sup> and giving rise to a complex interplay of applicable normative frameworks.

---

<sup>47</sup> See Jeevan Joseph, Akshara Anilkumar, Treesa Thomas, Binny S, ‘Discord: An all in one messaging application (Case Study)’, International Journal of Engineering Technology and Management Sciences, Issue: 5 Volume No.6 August-September 2022).

<sup>48</sup> Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC.

From the application of the DSA would derive, among other things, the prohibition of profiling minors in art. 28(2) DSA,<sup>49</sup> which would be difficult to comply with where the video game records the conversations of minors and consequently proposes targeted advertising to them, intercepting their consumption needs, as occurred precisely in the aforementioned Fortnite case.

The attention is bound to return to the protection of personal data collected in the context of conversations, which could be recorded: it is no coincidence that in 2020, Sony announced that the PlayStation 5, to be released shortly, would record conversations between players for the purposes of moderating them within gaming groups.<sup>50</sup> Conversations, written or audio, could in fact be recorded or saved by many video games, without them being provided with complete information, which clarifies, for example, the recording methods and retention times, as well as specific, compliant with the more stringent requirements already provided for by the GDPR.

Moreover, the game-based advertising aimed at minors could further integrate an unfair business practice; for that reason alone, it is prohibited and sanctioned. This has also been confirmed by the recent intervention of the European Commission, which has announced an action aimed at probing alleged unfair practices in the video game “Star Stable Online”, targeting in-game purchases aimed at children.<sup>51</sup> Star Stable is a children's video game where players explore an online world by riding horses and competing with friends in obstacle races. However, players who spend real money gain advantages within the game. To acquire items, players must exchange real money for in-game currency, known as “star coins”.

Therefore, the Commission, in collaboration with the Consumer Protection Cooperation Network, has requested information from the Swedish game developer of Star Stable to understand its commercial practices. As highlighted in the EC statement, the upcoming Digital Fairness Act may include stricter rules on virtual

---

<sup>49</sup> Although the formulation of this provision is not that clear. See Guido Scorza, ‘Digital services act. Le luci e le poche ma gravi ombre delle nuove regole UE’, in *agendadigitale.it*, April 28 2022.

<sup>50</sup> See the news released on October 17, 2020 on the website <https://gaming.hwupgrade.it/>, and the official statement, dated October 16, 2020, by Catherine Jensen, President of the “Global Consumer Experience” Division <https://blog.playstation.com/2020/10/16/details-on-new-voice-chat-functionality-coming-to-ps5/>, which does not deny the activation of the functionality in question and, indeed, even highlights the technical impossibility of deactivating it, while declaring it generically compliant with the regulations on privacy.

<sup>51</sup> See at [https://ec.europa.eu/commission/presscorner/detail/en/ip\\_25\\_831](https://ec.europa.eu/commission/presscorner/detail/en/ip_25_831).

currency transparency and fairness, and a crucial goal is “to ensure a safe online environment for consumers, particularly children, so they can enjoy gaming without facing unfair practices”.<sup>52</sup>

And last but not least, there are serious dangers of grooming for the minor when interfacing with other users, even adults, who may come into possession of important information relating to the minor, as well as the risks of becoming a victim of conduct that can be classified as cyberbullying.

In this regard, the EU Directive 2011/93 on combating the sexual abuse and sexual exploitation of children and child pornography<sup>53</sup> should therefore come into play, also in combination, in the Italian legal system, with Law No. 71 of 2017, aimed at preventing and combating the phenomenon of cyberbullying specifically, as well as the recent Law No. 70/2024, which also contains provisions aimed at preventing and combating the phenomena of both bullying and cyberbullying.

## 6. Tentative conclusions

In seeking to articulate some necessarily provisional conclusions, it must be acknowledged that, in the context of minor users of video games, the constellation of legal issues emerging is both multifaceted and conceptually intricate. The foundational premise is that minors constitute a structurally vulnerable category of users vis-à-vis smart technologies that may use AI-based applications, including but not limited to interactive entertainment systems. The spectrum of protective measures that may be envisaged is inherently differentiated and stratified.

At the outset, it should be observed that the existing regulatory landscape is characterised by a high degree of normative fragmentation. As the previous analysis has shown, the applicable framework at the European level is both complex and polycentric: multiple instruments converge, at times partially overlapping, thereby generating interpretative uncertainty and a consequent deficit in legal certainty.

---

<sup>52</sup> See the news published on March 21<sup>st</sup> 2025: <https://www.euronews.com/next/2025/03/21/european-commission-targets-in-game-currency-in-childrens-video-games>.

<sup>53</sup> This Directive should be overcome soon, considered the recent Proposal for a Directive on combating the sexual abuse and sexual exploitation of children and child sexual abuse material and replacing Council Framework Decision 2004/68/JHA.

Although some specificities emerge from the national legislation, they cannot mitigate the complexity nor, obviously, detach from the European legislation.

What emerges clearly is the limited sensitivity of the European legislator to the specificities of the phenomenon. This does not mean that no rules are provided as regards the protection of minors, but rather that they still adopt a ‘flattened view’ of the minor. In particular, neither the AI Act nor the Digital Services Act takes into account the evolving capacity of a minor in relation to his or her degree of maturity. Some positive hints come from another set of interventions: the GDPR, as well as the Italian national legislation—albeit through interpretative approaches that are at times complex—allows for an assessment and recognition of a minor’s capacity prior to reaching the age of majority. In particular, the GDPR proves instrumental from a contractual perspective, as it permits recognition of the ability to provide consent and, consequently, to enter into contractual obligations in the field of digital services, even for individuals who have attained the age of fourteen.

The true lever that enables the attribution of legal capacity to minors is therefore the notion of discernment, which is already firmly established as a principle at the international level. Yet, it must be observed that the capacity for discernment is conceptually distinct from the capacity to act. The former, in fact, is a principle whose primary foundation lies in the minor’s freedom of expression, and which finds its principal application within the realm of public law, notably in procedural matters — as an expression of the right to be heard — and, more broadly, in all matters involving minors. What is required, however, is a rearticulation of the notion of discernment, primarily by applying it to intra-family relationships, wherein the minor should be able to express personal inclinations and aspirations, which ought to guide his or her upbringing.

Furthermore, the capacity for discernment constitutes a general principle that requires implementation through indicators and criteria laid down by the legislature. In this regard, some practical tools already available may become effective: the so-called Pan-European Game Information (PEGI) standard may serve as useful benchmark for industry operators willing to acknowledge varying levels of maturity and discernment among the minor user base, and to introduce corresponding distinctions regarding the suitability of video games. After all, the fundamental freedom of expression is also manifested in the recreational sphere, particularly through the use of video games.

The PEGI system is, indeed, a method of rating video games based on age. Available guidelines classify video games into five age categories (+3, +7, +12, +16, +18) and eight content descriptors (bad language, discrimination, drugs, fear/horror, gambling, sex/nudity, violence, in-game purchases), in order to determine the games most suitable for minors. However, as noted, such indications often go largely unnoticed, resulting in the risk that minors may play video games unsuitable for their age, both in terms of content and visual elements.<sup>54</sup>

In parallel, recourse to soft law instruments, such as codes of conduct, has been explicitly endorsed at the European level as a regulatory modality of preference in this sector. This is exemplified by the Resolution adopted by the European Parliament on 18 January 2023, entitled “Consumer protection in online video games – a European Single Market approach”, which advocates for the elaboration of harmonised governance strategies capable of reconciling market integration with the imperative of child protection.

Moreover, notwithstanding the aforementioned lack of attention to the evolving maturity of minors within the AI Act, a crucial element can nonetheless be discerned in the notion of “AI literacy” as enshrined in Article 4 thereof. According to this provision, providers and deployers of AI systems shall take measures to ensure not only a sufficient level of AI literacy among their staff and other persons involved in the operation and use of AI systems on their behalf, but also to consider the persons or groups of persons on whom the AI systems are to be used. Consequently, providers will need to specifically assess and, where appropriate, provide training tailored to the audience on which their system is intended to have an impact. Particular attention should be given to systems that are, or could be, intended for use by minors. In such cases, the literacy requirement should be significantly elevated, due to the increased risks associated with the inherent vulnerability of the individuals concerned.

If rigorously implemented, this normative apparatus could operate as a catalyst for the epistemic empowerment of minors in their interaction with technological ecosystems, thereby attenuating informational asymmetries and mitigating the

---

<sup>54</sup> See T. Casadei and C. Coniglione, *Patti educativi digitali: come indirizzare i ragazzi a un uso consapevole dei device*, in [www.agendadigitale.it](http://www.agendadigitale.it), November 13<sup>th</sup> 2023.

manipulative potential of dark patterns. The correlative risk, however, concerns the distributive implications of such regulatory prescriptions, which risk engendering disproportionate compliance burdens for economic operators within the interactive entertainment industry.

Against this backdrop, an ancillary — yet significant — trajectory emerges: the systematic investment in training and awareness-raising initiatives, conceived not merely as auxiliary measures but as constitutive components of a governance architecture predicated upon inclusion rather than exclusion.

Such an approach would resonate with the foundational principle of proportionality, ensuring that minors — particularly those approaching the threshold of majority — are not unjustifiably marginalized from the digital entertainment sphere.



## A STORY OF AND FOR CHILDREN: THE LIFECYCLE LOOP OF CHILD RIGHTS-BASED AI

Sara Tibidò, Nadia Spatari, Sara Lilli e Maria Vittoria Zucca\*

### Abstract

This paper traces the lifecycle loop of child rights-based AI - from the initial phase of design through development and deployment - while mapping the ethical and regulatory landscape surrounding AI technologies designed for, accessed by, or impacting children. Building on established frameworks, the study advocates for the implementation of regulatory sandboxes and risk assessment measures to protect children's rights and interests against threats and emerging cyber risks. This research argues for the essential integration of a child rights-based approach at every stage and phase of an AI system's lifecycle, asserting that this leads to the development and deployment of more secure, child-centered systems.

### Table of Contents

A STORY OF AND FOR CHILDREN: THE LIFECYCLE LOOP OF CHILD RIGHTS-BASED AI .....	237
Abstract.....	237
Keywords.....	238

---

\* Sara Tibidò, Ph.D. Student in *Cybersecurity*, University of Bari “Aldo Moro” and IMT School for Advanced Studies Lucca, ORCID: 0009-0004-0646-0558.

Nadia Spatari, Ph.D. Student in *Cybersecurity*, National Inter University Consortium for Informatics (CINI) and IMT School for Advanced Studies Lucca. ORCID: 0009-0009-4935-7135.

Sara Lilli, Ph.D. Student in *Cybersecurity*, Sant’Anna School of Advanced Studies in Pisa and IMT School for Advanced Studies Lucca. ORCID: 0009-0000-2796-3067.

Maria Vittoria Zucca, Ph.D. Student in *Cybersecurity*, Sant’Anna School of Advanced Studies in Pisa and IMT School for Advanced Studies Lucca, ORCID: 0009-0004-0049-9611.

Double blind peer-reviewed contribution.

1. Starting the lifecycle loop of child rights-based AI .....	238
2. <i>Design and develop</i> : towards clear and practical child rights-based guidelines for practitioners.....	243
3. <i>Testing and validation</i> : regulatory sandbox environments to ensure safety and compliance.....	251
4. <i>Deployment</i> (and <i>post-deployment</i> ): cyber-threats and risk-driven mitigation.....	256
5. Closing the lifecycle loop of child Rights-Based AI.....	261

## **Keywords**

Artificial Intelligence - Children's rights - Children-centred AI - Digital Safety - Child Impact Assessment - Regulatory Sandbox

### **1. Starting the lifecycle loop of child rights-based AI**

Once upon a time, there was a doll named Cayla<sup>1</sup>, designed to be a friendly playmate for children. But behind her smiling face and sweet voice, she hides the potential of *listening* - and *sharing*. What was meant to be an AI embedded toy became a warning story of how innovation can overlook safety, privacy, and the fundamental rights of

---

<sup>1</sup>See the articles from BBC, 'German parents told to destroy Cayla dolls over hacking fears', (BBC News , 17 February 2017) <https://www.bbc.com/news/world-europe-39002142> accessed 06 July 2025; and World Economic Forum (WEF), 'Generation AI: What happens when your child's friend is an AI toy that talks back?' ( World Economic Forum, 22 May 2018) <https://www.weforum.org/stories/2018/05/generation-ai-what-happens-when-your-childs-invisible-friend-is-an-ai-toy-that-talks-back/> accessed 06 July 2025; other relevant cases should also be considered, such as the chatbots Wysa and Woebot, for which reference can be made to the following article: Geoff White, 'Child advice chatbots fail to spot sexual abuse' BBC (London, 11 December 2018),<https://www.bbc.com/news/technology-46507900> accessed 06 July 2025; and Karen Brown, 'Something Bothering You? Tell It to Woebot. When your therapist is a bot, you can reach it at 2 a.m. But will it really understand your problems?', *The New York Times* (New York, 01 June 2021), <https://www.nytimes.com/2021/06/01/health/artificial-intelligence-therapy-woebot.html> accessed 06 July 2025.

the youngest users. Cayla's conversations have indeed been found vulnerable to hacking, allowing strangers to listen and communicate directly to children.

While significant steps have been undertaken to improve safety and protection from similar situations (for instance, the adoption of *privacy*- and *security*-by-design approaches) different international organizations and associations, like UNICEF<sup>2</sup> and the Institute of Electrical and Electronics Engineers - IEEE<sup>3</sup>, and international non-governmental organizations (NGOs), such as the 5Rights foundation<sup>4</sup><sup>5</sup>, are calling for stronger, child-specific measures. These measures underscore the importance of integrating children's rights from the outset of the innovation process, ensuring their safety, protection, and participation.

While children should not be excluded from the digital world, as also stated by the UN General Comment No.25<sup>6</sup>, they should be protected by the risks (both *old* and *new*) they may face when using digital products or services. To move towards a welcoming, as well as more safe and secure digital ecosystem for children, it is crucial to integrate children's rights - along with safety and security measures - from the very beginning of the innovation process. This approach is particularly important when developing AI systems<sup>7</sup>. Indeed, the interaction between children and AI systems is

---

<sup>2</sup> UNICEF - V. Dignum, M. Penagos, K. Pigmans and S. Vosloo, 'Policy Guidance on AI for Children (Version 2.0)' (November 2021). <https://www.unicef.org/innocenti/reports/policy-guidance-ai-children> accessed 12 May 2025.

<sup>3</sup> IEEE Std 2089-2021, 'IEEE Standard for an Age Appropriate Digital Services Framework Based on the 5Rights Principles for Children' (vol., no., pp.1-54, 30 Nov. 2021). DOI: <https://doi.org/10.1109/IEEESTD.2021.9627644>.

<sup>4</sup> Digital Futures Commission and 5Rights Foundation, 'Child Rights by Design' (11 March 2023). <https://5rightsfoundation.com/resource/child-rights-by-design/> accessed 04 July 2025.

<sup>5</sup> 5Rights Foundation, 'Children & AI Design Code' (March 2025). <https://5rightsfoundation.com/children-and-ai-code-of-conduct/> accessed 04 July 2025.

<sup>6</sup> UN Committee on the Rights of the Child, 'General comment No. 25 (2021) on children's rights in relation to the digital environment' (02 March 2021) CRC/C/GC/25.

<sup>7</sup> Acknowledging that there is no internationally shared definition, for the purpose of this paper, we intend an "AI system" as defined by Article 3(1) of the EU AI Act and as further explained by the European Commission (February 2025) in its guidelines on AI systems definition (available online

complex and not limited only to those systems designed *for* children to be the main end users (*e.g.*: AI-enabled toys or systems used in the EdTech field), but also to those systems not meant for them but with which they *interact* in everyday lives contexts (*e.g.*: smart home assistant or recommender systems in social media and streaming platforms), and systems that can directly or indirectly *impact* them (*e.g.*: AI systems used to support decision process of social workers dealing with case of child maltreatment<sup>8</sup>)<sup>9</sup>. Attention should also be paid to factors that can influence AI's impact on children, such as socioeconomics, geographic and cultural context and norms, as well as other elements like children's developmental stages related to their physical, cognitive, emotional and psychological capacities.<sup>10</sup>

Accordingly, this story begins far back in the innovation process, from the discovery phase through the design and development phases, and it is grounded in the children's rights as defined by the UN Convention on the Rights of the Child (UNCRC). Indeed, since its adoption by the UN General Assembly in 1989 and its entry into force in September 1990, the UNCRC has become the world's most widely ratified human rights treaty<sup>11</sup>. With its ratification, States are legally bound to respect, protect, and fulfill the rights as outlined in the Convention<sup>12</sup>. Therefore, although the digital environment and new technologies may pose new challenges, the Convention (guided in its implementation in relation to the digital environment by the UN General Comment No.25) can still be considered an authoritative source on children's rights.

---

at: <https://digital-strategy.ec.europa.eu/en/library/commission-publishes-guidelines-ai-system-definition-facilitate-first-ai-acts-rules-application> - accessed 14 March 2025).

<sup>8</sup> See, for example, A. Kawakami and V. Sivaraman, and L. Stapleton, and H.F. Cheng, and A. Perer, and Z.S. Wu, and H. Zhu, and K. Holstein, "Why Do I Care What's Similar?" Probing Challenges in AI-Assisted Child Welfare Decision-Making through Worker-AI Interface Design Concepts' (ACM Designing Interactive Systems Conference, online, 13-17 June 2022).

<sup>9</sup> UNICEF - V. Dignum, M. Penagos, K. Pigmans and S. Vosloo (November 2021).

<sup>10</sup> *Ibidem*.

<sup>11</sup> UNICEF, 'How the Convention on the Rights of the Child works' <https://www.unicef.org/child-rights-convention/how-convention-works> accessed 12 May 2025.

<sup>12</sup> *Ibidem*.

In 2011, the UN Human Rights Council endorsed the “Guided Principles on Business and Human Rights” (UNGPs)<sup>13</sup>, implementing the 2008’s UN “Protect, Respect and Remedy” framework for business and human rights and recognizing business's responsibility to respect also those rights as enshrined in the UNCRC<sup>14</sup>. The UNGPs ‘*are applied to the digital context through the UN Human Rights B-Tech Project*’<sup>15</sup> (e.g.: the briefing, conducted together with UNICEF and published in 2024, on “Taking a Child Rights-Based Approach to Implementing the UNGPs in the Digital Environment” unpacks core headlines on the implementation of UN principles with a child rights perspective<sup>16</sup>). A year later, in 2012, UNICEF, the UN Global Compact and Save the Children developed the “Children’s Rights and Business Principles”, a range of actions companies can undertake in different contexts to respect and support children’s rights<sup>17</sup>. Although those Principles do not constitute a legally binding document, they are instruments of soft law that have been ‘*incorporated or referenced in legislation, industry codes of conduct, and market-entry requirements in various sectors of the economy, including the digital sector*’<sup>18</sup>.

Unlike such voluntary approaches, the European Union has imposed some legal obligations to online intermediaries and platforms. In particular, first in 2018 with the “Audiovisual Media Services Directive” (AVMSD), coordinating national legislations and setting out responsibilities for media service providers (e.g.: protection of users, children in particular, from certain kinds of content or programs and establishment

---

<sup>13</sup> UN, ‘Guided Principles on Business and Human Rights’ (01 January 2012) 978-92-1-154201-1.

<sup>14</sup> *Ibidem*.

<sup>15</sup> OECD, ‘Shaping a Rights-Oriented Digital Transformation’ (28 June 2024), No. 368, OECD Digital Economy Papers (citing). [https://www.oecd.org/en/publications/shaping-a-rights-oriented-digital-transformation\\_86ee84e2-en.html](https://www.oecd.org/en/publications/shaping-a-rights-oriented-digital-transformation_86ee84e2-en.html) accessed 12 May 2025.

<sup>16</sup> UNICEF and UN Human Rights, ‘Taking a Child Rights-Based Approach to Implementing the UNGPs in the Digital Environment’ (November 2024) <https://www.unicef.org/childrightsandbusiness/reports/b-tech-contribution> accessed 05 July 2025.

<sup>17</sup> UNICEF, the UN Global Compact and Save the Children, ‘Children’s Rights and Business Principles’ (2012) <https://www.unicef.org/documents/childrens-rights-and-business-principles> accessed 12 May 2025.

<sup>18</sup> OECD (28 June 2024), citing.

of age verification systems in video-sharing platforms)<sup>19</sup>, and then in 2022, with the “Digital Services Act” (DSA). The DSA, which refers to international standards (including the UNGPs)<sup>20</sup> and aims at regulating online platforms and intermediaries (to be specific: very large online platforms and search engine, online platforms, host services and intermediary services), contains some child-specific provisions (*e.g.*: Article 14 on comprehensible child-friendly explanations of conditions and terms of use, Article 28 on appropriate and proportionate measures to protect children’s safety, security and privacy, and Articles 34 and 35 on mandatory annual fundamental rights risks’ assessments and mitigation measures).<sup>21</sup>

Designing with children’s rights in mind is no simple task, but retrofitting a product to comply with these rights after development can be both difficult and costly.<sup>22</sup> Accordingly, this paper proposes a children’s rights-based approach to the entire AI system lifecycle, emphasizing the integration of children’s rights, needs, and perspectives - alongside safety, security, and stakeholders inputs - at every phase. The aim is to ensure that systems are well-designed from the outset to be compliant with children’s rights standards and obligations, thereby reducing the need for substantial post-deployment corrections. Therefore, the following sections will describe a story of innovation that begin from (i) the legal, policy and technical frameworks shaping the *design* and *development* phases of an AI system for/impacting/ accessed by children, passing through (ii) the phases of *testing* and *validation* with the use of regulatory sandboxes, to (iii) the phases of *deployment* and *post-deployment*<sup>23</sup>.

---

<sup>19</sup> *Ibidem*.

<sup>20</sup> *Ibidem*.

<sup>21</sup> OECD, ‘Towards digital safety by design for children’ (19 June 2024), No. 363, OECD Digital Economy Papers. [https://www.oecd.org/en/publications/towards-digital-safety-by-design-for-children\\_c167b650-en.html](https://www.oecd.org/en/publications/towards-digital-safety-by-design-for-children_c167b650-en.html) accessed 05 July 2025.

<sup>22</sup> Digital Futures Commission and 5Rights (11 March 2023).

<sup>23</sup> For the division of the phases constituting the AI system lifecycle, we recall the work of D. De Silva and D. Alahakoon, ‘An Artificial Intelligence Life Cycle: From Conception to Production’ (2022) 3(6) Patterns, <https://doi.org/10.1016/j.patter.2022.100489> accessed 12 May 2025. Indeed, the Authors consider an AI system’s life cycle made of three main phases: “*design*”, “*develop*” and “*deploy*”, each of them made of different “*stages*”. While the Authors do not consider a separate phase for testing and validation, in the “*deploy*” phase it is considered a “*post-deploy*” stage (stage no.16).

## **2. Design and develop: towards clear and practical child rights-based guidelines for practitioners**

State have the duty, under international human rights law, to protect people in their jurisdiction or/and their territory from human rights abuses, and corporate responsibility to respect human rights exists '*regardless of their size, sector, location, ownership and structure*'<sup>24</sup>. Therefore, States and businesses have different but complementary responsibilities<sup>25</sup>. Accordingly, since the exercise and protection of human rights can be affected by how '*digital technologies are designed, developed and deployed*', it is important to embed human rights in all the phases of an innovation process<sup>26</sup>. However, providing all stakeholders with clear, technically applicable and cross-cutting guidelines is challenging.

Before rights-specific considerations, ethical AI-related challenges have been a central topic of discussion among policy makers, professionals and academics. Indeed, ethical principles and guidelines have been found difficult to be integrated into the engineering process that power AI development: there is a critical gap between these principles, available guidelines and the realities of the engineering practice<sup>27</sup>. Moreover, the accountability gap, in terms of clarity about who should be ought accountable '*for the outcomes of technology use, to whom, and how*'<sup>28</sup>, presents a major challenge for engineers (e.g.: hierarchies of power in the workplace that may limit their

---

<sup>24</sup> UN, 'Guided Principles on Business and Human Rights' (01 January 2012), citing.

<sup>25</sup> *Ibidem*.

<sup>26</sup> OECD (28 June 2024), citing.

<sup>27</sup> IEEE SA, 'Report: Addressing Ethical Dilemmas in AI: Listening to Engineers Report' (2021) <https://standards.ieee.org/initiatives/autonomous-intelligence-systems/ethical-dilemmas-ai-report/> accessed 05 July 2025.

<sup>28</sup> *Ibidem*, citing.

technical and organizational choices; absence of independent infrastructures to turn to in case of ethical concerns or to report cases of non-compliance)<sup>29</sup>.

While various ethical principles have been proposed in relation to the rights of the child and AI systems, their effective implementations and practical applications are still mainly unexplored<sup>30</sup>. Children are different among them and from adults, accordingly AI principles concerning children should not be considered nor treated as a subcategory of other guidelines<sup>31</sup>. Accordingly, Wang *et al.* identify four main ‘challenges in translating ethical AI principles into practice for children’<sup>32</sup>:

1. ‘*Lack of consideration of the developmental aspect of childhood*<sup>33</sup>: the vast number of technologies and their various applications make it difficult to provide consistent professional codes and norms for AI applications. Incorporating children introduces a new layer of complexity to this scenario. Their unique needs, diverse age ranges, development stages, backgrounds, physical and psychological traits necessitate special attention;
2. ‘*Lack of consideration of the role of guardians in childhood*<sup>34</sup>: parent(s) or legal guardian(s) bear the ethical and legal primary responsibility for the upbringing and development of the child (Article 18 UNCRC) and for the children’s provision of appropriate direction and guidance in the exercise of their rights (Article 5 UNCRC). Therefore, the role of parent(s) and legal guardian(s) must be considered and examined, but without falling in the traditional assumption that they possess superior expertise or skills to orient children in the digital landscape;

---

<sup>29</sup> *Ibidem*.

<sup>30</sup> G. Wang, J. Zhao, M. Van Kleek & N. hadbolt, ‘Challenges and opportunities in translating ethical AI principles into practice for children’ (2024) *Nature Machine Intelligence* 6, 265–270 <https://doi.org/10.1038/s42256-024-00805-x> accessed 04 July 2025.

<sup>31</sup> *Ibidem*.

<sup>32</sup> *Ibidem*, citing.

<sup>33</sup> *Ibidem*, citing.

<sup>34</sup> *Ibidem*, citing.

3. ‘*Lack of child-centred evaluations considering children’s best interests and rights*’<sup>35</sup>: relying solely on quantitative metrics and technical evaluation, while important, can present challenges. Translating ethical AI principles into practice for children requires a more balanced approach between both empirical variables and quantitative measurements, and, in general, a paradigm shift towards a more human-centred approach;
4. ‘*Lack of a coordinated, cross-sector and cross-disciplinary approach*’<sup>36</sup>: experts from other domains, dealing with analogous issues, often have different vocabularies and methodologies. One of the main challenges lies in their adaptability across different AI principles. Cross-sector and cross-disciplinary collaboration is essential to harmonize and encourage knowledge transfer while avoiding duplicate efforts.<sup>37</sup>

These challenges add other layers of difficulty in integrating children’s rights in the design and development of a product or service. Smart toys like Cayla’s doll, should not only be secure- and privacy-by-design, but should also *e.g.* take into account children developing language skills, by adopting a child friendly language in accordance of the maturity of the child, while also considering a system of blocking access to content children should not access without adults’ supervision. Accordingly the difficulty is not just on how to make the system embedded in the toy technically robust and resilient, but it also concerns dealing with developmental theories, adaptability to different situations (*e.g.*: Is the system capable of adapting content and language according to the child’s specificity? and how to make the system able to do that while following the principle of data minimization?), and definitions of concept like “appropriateness” (*e.g.*: What may be considered appropriate for a child of a certain age, maturity and background could not be necessarily considered appropriate for and by another child).

Given all these challenges, engineers and practitioners working on the design and development of AI systems for, accessed by or impacting children, are required to

---

<sup>35</sup> *Ibidem*, citing.

<sup>36</sup> *Ibidem*, citing.

<sup>37</sup> *Ibidem*.

deal with more than technical problems and solutions. This is for those topics that are indeed ‘*socio-technical*’<sup>38</sup>, meaning that ‘*social and technical aspects are interwoven in such a way that studying one without due consideration of the other makes for an incomplete investigation and understanding*’<sup>39</sup>. To guide practitioners in diving this scenario, some references are made to existing contributions from academia, industry, international organizations/associations and NGOs.

However, academic contributions on how to design, develop and deploy AI systems compliant with related existing standards and obligations are still few, and mainly summarized as “design implications” at the end of a paper. While literature reviews can offer a valid overview of a topic, few are the works<sup>40</sup> investigating children’s rights coverage and inclusion in engineering and computer science’ works, and even less are works trying to summarize all these “design implications” in one single and easy to use document. This sum up could be interesting and possibly useful in real life situations, since coming from in-the-field studies, and a service- or product-specific framework can be valuable to achieve precise applicable guidelines.

Nevertheless, industry-partnership projects and international organizations and associations have been mainly focusing on a broader approach, advocating for responsible innovation for children well-being (e.g.: LEGO and UNICEF<sup>41</sup>), a child-centered approach to AI system (e.g.: UNICEF<sup>42</sup>) and age appropriate services (e.g.:

---

<sup>38</sup> Rashina Hoda., *Qualitative Research with Socio-Technical Grounded Theory. A practical guide to qualitative data analysis and theory development in the digital world* (Springer Cham, 2024), <https://doi.org/10.1007/978-3-031-60533-8> citing.

<sup>39</sup> *Ibidem*, citing.

<sup>40</sup> See, for example, G.Wang, J.Zhao, M.Van Kleek, and N.Shadbolt, ‘Informing Age-Appropriate AI: Examining Principles and Practices of AI for Children’ (CHI - Conference on Human Factors in Computing Systems, New Orleans, LA, April 30 – May 5 2022).

<sup>41</sup> UNICEF and LEGO, ‘The Responsible Innovation in Technology for Children (RITEC) Project’. See UNICEF’s webpage ‘Responsible Innovation in Technology for Children. Project | Digital technology, play and child well-being’ (UNICEF) <https://www.unicef.org/innocenti/projects/responsible-innovation-technology-children> accessed 06 July 2025.

<sup>42</sup> UNICEF - V. Dignum, M.Penagos, K.Pigmans and S.Vosloo (November 2021).

IEEE<sup>43</sup>). These contributions are one of the most cited when it comes to children and AI.

Contributions coming from (or in collaboration with) businesses and industry are important for their ground on real life scenarios and interests, bridging the gap between academic research and industry actual needs. Integrating a children's rights approach and design for well-being into business strategies can have positive outcomes for both children (their rights, needs and desire with better products) and brands (boosting brand reputation and values, by differentiating themselves from their competitors and within their customers, and attracting possible investors)<sup>44</sup>.

The “Responsible Innovation in Technology for Children” (RITEC) project is a collaboration between UNICEF and The LEGO Group, funded by The LEGO Foundation, aiming at investigating how the design of children's digital experiences affects their well-being, and provides guidance on design choices that can promote positive outcomes for children's well-being<sup>45</sup>. From the RITEC project a framework (the final “RITEC-8”, updated and published in 2024) and a design toolbox (the “RITEC Design Toolbox”) have been developed to provide an ‘*easy-to-use guidance for designers of digital play*’<sup>46</sup> by including a list of relevant features and examples<sup>47</sup>.

The framework developed in the context of this project is called RITEC-8<sup>48</sup> because is grounded in 8 pillars: (i) autonomy (allow children to be in control and make decisions that matter for them and their play); (ii) competence (considering

---

<sup>43</sup> IEEE, Standard for an Age Appropriate Digital Services Framework Based on the 5Rights Principles for Children, 2021. DOI: <https://doi.org/10.1109/IEEESTD.2021.9627644>.

<sup>44</sup> *Ibidem*.

<sup>45</sup> UNICEF, The Business Case for Designing for Children's Well-Being in Digital Play Summary for Executives, 2024. <https://www.unicef.org/childrightsandbusiness/reports/business-case-designing-childrens-well-being-digital-play> accessed 06 July 2025.

<sup>46</sup> *Ibidem*, citing.

<sup>47</sup> *Ibidem*.

<sup>48</sup> UNICEF, Digital technology, play and child well-being. Responsible innovation in technology for children, 2024. <https://www.unicef.org/innocenti/reports/responsible-innovation-technology-children> accessed 06 July 2025.

meaningful rewards for progress and allowing children to adjust and improve); (iii) emotions (experience positive as well as more challenging emotions); (iv) relationships (taking into account children's different needs and characteristics, allow them to make new friends and socialize while competing, creating, and/or collaborating with others); (v) creativity (encourage children's curiosity and imagination to invent and experiment); (vi) identities (while playing, allow children to explore and express facets of themselves and of others); (vii) diversity, equity & inclusion (experience intended for different children and needs); and (viii) safety and security (children feel and are kept safe while playing)<sup>49</sup>. The framework is also accompanied by a design toolbox (RDT) with the aim of providing design professionals in the online gaming industry (product, visual, UX, research, but also management levels, and safety professionals) with practical tools for incorporating the RITEC-8 for children's well-being into their design process<sup>50</sup>.

UNICEF, before the RITEC Project, has already been focusing on AI systems in its "Policy Guidance on AI for Children"<sup>51</sup>. The document provides nine requirements for child-centered AI, and furnishes a set of '*complementary online resources*' and '*practical implementation tools*'<sup>52</sup>. The guidance is addressed to different stakeholders, from development teams to policymakers, and, while this is important, finding a common both understandable and practical language for all may be challenging. The risk is too high-level guidance, resulting difficult to fully implement into the actual work's duties (e.g.: The "transparency" principle does not specify how to explain AI decisions to a child of a certain age or background over a child of another age or background).

Meanwhile, the IEEE, as technical professional organization, elaborated the "Standard for an Age Appropriate Digital Services Framework Based on the 5Rights

---

<sup>49</sup> *Ibidem*.

<sup>50</sup>UNICEF, 'RITEC Design Toolbox. Designing for children's well-being in digital play' <https://www.unicef.org/childrightsandbusiness/workstreams/responsible-technology/online-gaming/ritec-design-toolbox> accessed 06 July 2025.

<sup>51</sup> UNICEF - V. Dignum, M.Penagos, K.Pigmans and S.Vosloo (November 2021).

<sup>52</sup> *Ibidem*, citing.

Principles for Children”<sup>53</sup> (IEEE 2089-2021)<sup>54</sup>. The IEEE 2089-2021 is practical in its formulation, being developed to be used in ‘*software engineering and digital services organizations*’<sup>55</sup>, including but not limited to those ‘*providing services and products that engage with children or are likely to be accessed by or engage with children*’<sup>56</sup>. Although its technical nature, the document is informed by the UNCRC and the UN General Comment No.25, and it is based on the principle of the “*best interests*”<sup>57</sup> of the child<sup>58</sup>. The Document is an important attempt to combine a more technical approach with existing policies and regulations on the subject.

NGOs have also attempted ‘*bridging high-level principles and practical challenges*’<sup>59</sup> by defining what innovators need to know to realise children’s rights in their product or service<sup>60</sup>. In 2023, the “5 Rights Foundation” (within the “Digital Future Commission” project) released the “Child Rights By Design”: a guidance aiming to provide clear and practical indications to those figures involved in the process of

---

<sup>53</sup> IEEE Std 2089-2021(2021).

<sup>54</sup> In 2023, the IEEE 2089-2021 has been recognized to serve as the foundation for an *European Committee for Standardization (CEN)/European Committee for Electrotechnical Standardization (CENELEC)* Workshop Agreement (CWA 18016), helping to serve various EU regulations and policies, such as the the DSA and the ‘European strategy for a Better Internet for Kids (BIK+)’ (see: IEEE SA, ‘IEEE 2089™ Provides Foundation for European Reference Document for Children’s Protection & Well-being Online’ (2023). <https://standards.ieee.org/news/ieee-2089-european-reference-document/> accessed 13 May 2025).

<sup>55</sup> IEEE Std 2089-2021 (2021), citing.

<sup>56</sup> *Ibidem*, citing;

<sup>57</sup>The “best interest” principle refers to Article. 3 UNCRC and, according to S. Livingstone et al. (S. Livingstone, N. Cantwell, D.Özkul, G. Shekhawat and B. Kidron, ‘The best interests of the child in the digital environment’ (March 2024) <https://www.digital-futures-for-children.net/our-work/best-interests> accessed 14 May 2025), it implies that, when children’s rights seem to be in tension or when other parties’ interests (such as those of companies or organizations) may conflict with them, to identify “*which rights are to be given precedence*”, an independent procedure of “*best interests’ determination*” should be designed to avoid “*provide legitimization for whichever right a company may favour*”.

<sup>58</sup> IEEE Std 2089-2021 (2021).

<sup>59</sup> Digital Futures Commission and 5Rights (11 March 2023).

<sup>60</sup>*Ibidem*.

creation, design, development and deployment of a digital product or services likely to be used by or impacting on children<sup>61</sup>. Grounded on the UNCRC, the guidance calls for a “*by-design*” approach<sup>62</sup>, that would mean including children's rights considerations in every phase of an AI system's lifecycle. By collecting inputs from innovators, practitioners, and children, the guide is structured around 11 high-level principles<sup>63</sup> and align with the main crucial phases of an innovation process<sup>64</sup>. Given the peculiar opportunities and challenges AI systems pose, the 5Rights Foundation also published the “Children and AI Design Code. A protocol for the development and use of AI systems that impact children”<sup>65</sup>(2025). The Code is composed of distinct stages and developed so as to be applicable in each phase of an AI system's lifecycle<sup>66</sup>. Moreover, it is structured as an ‘*assessment process*’ so that ‘*non-conformity is identified, evaluated, and mitigated*’<sup>67</sup> and progress are recorded in writing<sup>68</sup>. While recording can help keep track of both progress and risks, the “*requirement checklist*” provided at the end of the Code may be not sufficient to report and elaborate both of them. Here, integrating existing related initiatives can be a valuable asset and can avoid “reinventing the wheel” when other contributions or disciplines have already found a solution (as suggested by Wang et al. when calling for a cross-sector and

---

<sup>61</sup>*Ibidem.*

<sup>62</sup>As C. Djeffal highlights (in: C.Djefal, ‘Children's Rights by Design and Internet Governance: Revisiting General Comment No. 25 (2021) on Children's Rights in Relation to the Digital Environment’ (2022) 11(6) Laws <https://doi.org/10.3390/laws11060084> accessed 05 July 2025), the “*by-design thinking*” has traditionally been applied in the area of privacy, data protection, and security, but it has begun to spread also throughout the legal system. The “*law-by-design norms*” take advantage of “*the law's binding nature and combine it with normative claims that are to be translated into technology*”.

<sup>63</sup>5Rights Foundation's “Child Rights by Design” principles: (i) equity and diversity, (ii) best interests, (iii) consultation, (iv) age appropriate, (v) responsible, (vi) participation, (vii) privacy, (viii) safety, (ix) wellbeing, (x) development, and (xi) agency.

<sup>64</sup>Digital Futures Commission and 5Rights (11 March 2023).

<sup>65</sup> 5Rights Foundation (March 2025).

<sup>66</sup> *Ibidem.*

<sup>67</sup> *Ibidem*, citing.

<sup>68</sup> *Ibidem*.

cross-disciplinary approach). The IEEE 2089-2021<sup>69</sup>, for example, foresees the creation of an '*Age Appropriate Register (AAR)*'<sup>70</sup>: a '*medium*'<sup>71</sup>, used to document and communicate progressively, and '*handover*'<sup>72</sup> between the competences and responsibilities of the stakeholders involved in one phase to those involved in the subsequent phases<sup>73</sup>. Therefore, the AAR (or a similar tool), can be an important ally in monitoring and ensuring compliance with children's rights (and safety and security standards) throughout the whole AI system's lifecycle.

Whether the use of this or similar tools, in cases such as the doll Cayla, could have been found useful and successful in timely identifying, analysing, and mitigating risks and challenges remains an open question. Further research is needed in order to assess the practical outcomes of applying such frameworks and guidelines, so as to provide effective and actionable indications to practitioners. Retrofitting a product to comply with these rights after development can be equally (if not more) difficult and costly.<sup>74</sup> Accordingly, a child rights approach should be kept as a lighthouse since the pre-deployment phase of an AI system's lifecycle.

### **3. Testing and validation: regulatory sandbox environments to ensure safety and compliance**

Testing AI systems intended for children within regulatory sandboxes is a crucial step in ensuring the protection of their rights. Children and preadolescents, as particularly vulnerable users, require special consideration from the earliest stages of technology

---

<sup>69</sup> IEEE Std 2089-2021(2021).

<sup>70</sup> *Ibidem*, citing.

<sup>71</sup> *Ibidem*, citing.

<sup>72</sup> *Ibidem*, citing.

<sup>73</sup> *Ibidem*.

<sup>74</sup> Digital Futures Commission and 5Rights (11 March 2023).

design. It is essential to assess how these systems might affect their privacy, safety, and overall well-being from the outset.

Regulatory sandboxes provide a controlled environment in which innovative digital solutions can be tested, allowing technological development to be balanced with the need for protection. This approach makes it possible to identify and address potential issues before the product is released to the market and its compliance with standard and regulation children's rights by design. Several European States include the use of sandboxes as a means to build a comprehensive legal framework for AI. This trend is supported by the EU, which views regulatory sandboxes as facilitators of innovation and recognizes them as a crucial tool in future regulatory activities concerning AI. A regulatory intervention for the definition of this tool was provided by the AI Act, definitively approved on May 21, 2024, which in Article 57 defines AI sandboxes<sup>75</sup>. Regulatory sandboxes on AI, established by European or national competent authorities, provide a controlled environment to develop and test innovative AI systems before commercial deployment. These activities take place under the direct supervision of authorities to ensure compliance with EU and national regulations. When the systems involve the processing of personal data or fall under other regulated areas, data protection authorities and other relevant bodies must be involved in the sandbox's operation<sup>76</sup>. Regulatory sandboxes can help address these issues by providing regulatory certainty for technology companies and other stakeholders, fostering collaboration and capacity-building with and among regulators, and promoting regulatory clarity and compliance<sup>77</sup>.

The use of regulatory sandboxes in Europe to test products aimed at minors is still limited and not yet systematized. However, there are some cases and emerging trends that indicate a growing interest in this area, particularly in relation to financial

---

<sup>75</sup>EU, 'Artificial Intelligence Act' (2024). Chapter VI: Measures in Support of Innovation. <https://artificialintelligenceact.eu/chapter/6/> accessed 12 May 2025.

<sup>76</sup> S. Ranchordas, 'Experimental Regulations for AI: Sandboxes for Morals and Mores' (2021) 1(1) *Morals & Machines* 86 [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=3839744](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3839744) accessed 12 May 2025.

<sup>77</sup> Datasphere Initiative, 'Sandboxes for data: creating spaces for agile solutions across Borders' (2022) <https://www.thedatasphere.org/> accessed 12 May 2025.

education for young people, the protection of personal data (including GDPR compliance and age of consent requirements), the responsible use of technology such as AI and digital platforms designed for minors, and the development of secure digital payment solutions for those under the age of 18.

Datasphere initiative<sup>78</sup> has published a case study on regulatory sandboxes, highlighting the inability of current laws and policies to keep pace with rapid technological developments. The study proposes regulatory sandboxes as tools to foster innovation while ensuring effective data governance - particularly when it comes to children's data. The sandbox model described in the study does not allow for temporary suspensions of legal constraints; instead, it promotes innovation within the existing regulatory framework, encouraging solutions that remain compliant with current rules, trends and better oversee foreign products that process children's data within their jurisdictions<sup>79</sup>.

The Norwegian Police University College has tested a bot ("PrevBOT") within a regulatory privacy sandbox, aiming to explore the feasibility of developing a tool capable of automatically patrolling the open internet. The goal of this project is to detect and prevent the sexual exploitation of minors by identifying suspicious behavior and grooming attempts in real time. By combining AI-driven language analysis, behavioral profiling, and age estimation technologies, PrevBOT seeks to serve as a proactive digital safeguard, helping law enforcement intervene before harm occurs - while operating within strict privacy and ethical frameworks. PrevBOT is designed to protect minors online by addressing the growing issue of digital grooming. This crime involves adults who use psychological manipulation and digital communication to build trust with children, often with the intent of sexual exploitation. To effectively counter this threat, PrevBOT integrates advanced technologies capable of identifying risky interactions before they escalate. The system is trained to detect grooming language not only in explicit terms but also in the subtle

---

<sup>78</sup> The "Datasphere Initiative" is a non-profit dedicated to global collaboration on technical and policy solutions for the urgent, multidimensional, and cross-border challenges of data governance (see: <https://www.thedatasphere.org//about-us/> accessed 14 May 2025).

<sup>79</sup> UNICEF, 'Regulatory sandboxes . Case study', 2025: <https://www.unicef.org/innocenti/media/11091/file/UNICEF-Innocenti-Regulatory-Sandboxes-Case-Study-2025.pdf> accessed 14 May 2025.

and coded language often used in chats, including slang and emerging online expressions. It can analyze conversation patterns to recognize early signs of inappropriate behavior, even when the language appears innocent. In addition, PrevBOT estimates the age and gender of users based on their writing style and digital behavior. This allows it to identify potentially fake profiles, especially when adults pretend to be minors to gain access to youth-oriented spaces. Recognizing age discrepancies is important for detecting interactions where children may be at risk. The bot also performs sentiment and behavioral analysis by monitoring response times, typing speed, emotional tone, and interaction patterns. This helps identify users who, despite maintaining a calm or friendly appearance, may be displaying signs of persistence, or manipulation - indicators that their intentions might not align with their words. Together, these capabilities enable PrevBOT to provide proactive protection for minors, flagging dangerous behavior early while respecting privacy regulations and promoting safer digital environments for young users<sup>80</sup>. PrevBOT project is still in its early stages, and it will be interesting to see how it manages to strike a balance between the need for freedom and the need for safety. Minors have a right to agency and privacy, but without an adequate level of online protection, they would not be able to fully exercise those rights. Trust is a key element for a project that aims to comply with both current regulations and the principles of ethical and responsible AI. In this regard, emphasizing transparency and actively involving stakeholders throughout the research process provides a strong foundation.

An important experimentation to make in consideration is the case of the UK's ICO Regulatory Sandbox. The United Kingdom's Information Commissioner's Office (ICO) established the ICO Sandbox program in 2019 to support organizations developing innovative data-based products and services, ensuring compliance with privacy regulations. Since 2020, the program has focused particularly on two areas: protecting children's online privacy through the Children's Code and managing the complex sharing of personal data in sensitive sectors such as health, education, finance, and public administration.

---

<sup>80</sup> The Norwegian Police University College, exit report: PrevBOT (20 September 2024) <https://www.datatilsynet.no/en/regulations-and-tools/sandbox-for-artificial-intelligence/reports/the-norwegian-police-university-college-exit-report-prevbot/> accessed 14 May 2025.

A notable example is the Lookafterme project by FlyingBinary Limited<sup>81</sup>, a digital service based on AI designed to support mental health issues such as anorexia and bulimia, including for children from the age of eight. The system monitors online content in real time and alerts users to potentially harmful material, providing integrated clinical support. During its participation in the Sandbox, FlyingBinary ensured full compliance with UK GDPR, the Data Protection Act 2018, and the Children's Code. The company focused particularly on secure and age-appropriate authentication methods for children, the principle of data minimization, and data protection by design. Special attention was given to the protection of health data, considered sensitive, and ensuring that data processing always took place in the best interest of the child, using the "Best Interests Framework", an ICO tool inspired by the UNCRC. The project serves as a replicable model demonstrating how technological innovation and the protection of fundamental rights can be effectively integrated, especially in sensitive fields like health and education.

Lessons learned from various sandbox experiences highlight both their potential and the challenges they pose - especially concerning children's data. Sandboxes can play a crucial role in helping stakeholders balance the benefits of using minors' data with the need to fully safeguard their rights: testing the doll Cayla in such an environment could have helped experts identify those vulnerabilities and issues before its deployment into the market, and possibly avoid children's harm and company's reputational damage. Encouraging tech companies to participate in sandboxes is a key factor in their success. While some sandboxes provide financial support to cover legal, technical, or operational costs, the most valuable incentive is often the regulatory clarity and compliance assurance they offer.

Sandboxes have demonstrated global relevance and potential for cross-border replication. In particular, international sandboxes can enhance regulatory capacity, improve cooperation, foster innovation and compliance, and promote the availability and accessibility of data across jurisdictions and sectors. By engaging directly with emerging technologies - including those developed abroad regulators, especially in countries without a strong domestic tech sector, can stay informed on global trends

---

<sup>81</sup> Information Commissioner's Office, 'Regulatory sandbox final report: Flyingbinary' (Tech. Rep., 2022). <https://ico.org.uk/media2/migrated/4021302/flyingbinary-exit-report-202208.pdf> accessed 15 May 2025.

and better oversee foreign products that process children's data within their territory<sup>82</sup>.

#### **4. Deployment (and post-deployment): cyber-threats and risk-driven mitigation**

The deployment of AI-based technologies designed for/interacting with/impacting children does not mark the end of the innovation lifecycle but initiates a new phase - one that requires ongoing oversight, responsiveness and ethical commitment. Indeed, ensuring that these systems uphold children's rights over time requires a structured post-deployment framework of assessment, monitoring, and risk mitigation.

interference and, in fact, prove to be particularly vulnerable to a wide range of cyber-threats.<sup>83</sup> Common risks include data breaches that can compromise sensitive personal information (e.g.: names, locations and voice recording) or even adversarial attacks that can manipulate system inputs to trigger inappropriate or unsafe outputs, distorting educational content or conversational responses.

As concerns data breaches, particular attention should be paid to the real case of the Smart Toy produced by Fisher-Price<sup>84</sup>. This product represents one of the earliest and most emblematic examples of an Internet-connected smart toy, designed to establish personalized interaction with the child through the use of a rudimentary form of AI<sup>85</sup>. Manufactured by the American company Fisher-Price, a subsidiary of Mattel, the toy was available in three versions - a bear, a monkey, and a panda - and relied on Wi-Fi connectivity and a mobile application managed by parents to oversee its functions. The Smart Toy was capable of gradually learning the child's preferences, customizing

---

<sup>82</sup> *Ibidem*.

<sup>83</sup> For further reading, S. Shasha et al, 'Playing with Danger: A Taxonomy and Evaluation of Threats to Smart Toys' (2018) 6 IEEE Internet of Things Journal 2986, 2996.

<sup>84</sup> Description of the Fisher-Price Smart Toy Bear, see: <http://fisher-price.mattel.com/shop/us/fp/smart-toy/smart-toy-bear-dnv31>.

<sup>85</sup> For a more in-depth look at the case, refer to: M.C. Gaeta, 'Smart toys and minors' protection in the context of the Internet of everything' (2020) 11(2) Eur J Privacy L & Tech 118.

its content and responses through the use of physical smart cards<sup>86</sup>. However, a technical analysis conducted at the hardware, software and network levels<sup>87</sup> revealed critical vulnerabilities in the system's APIs - the *Application Programming Interfaces* that enable communication between applications and services. These vulnerabilities involved the lack of proper identity verification for message senders, thereby allowing unauthorized third parties to gain access to sensitive personal data, such as the child's name, date of birth, language, activity history, and similar information. More concerning was the demonstrated possibility of modifying or deleting user profiles and even altering the toy's functionality, potentially exposing children to physical and psychological harm. This case highlights how, even in the absence of immediate damage, a cyberattack can deeply compromise a child's private and relational sphere, emphasizing the risks posed by the aggregation of seemingly innocuous data, which can be utilized to construct a detailed and exploitable personal profile.

As for the cyber-risks of manipulation, some smart toys have begun incorporating generative AI systems such as ChatGPT - one notable example is Grok<sup>88</sup>. Grok is a conversational toy designed to engage children through verbal interaction powered by a LLM, and it is among the first toys to feature a voice interface connected to ChatGPT. While the toy's goal is to promote natural dialogue, integrating LLMs into children's products raises significant concerns around safety and control. In Grok's case, researchers conducted an experiment<sup>89</sup> that demonstrated the toy continuously streams audio to external servers without requiring a wake word. It records not only

---

<sup>86</sup> Fisher-Price described the toy as “*an interactive learning friend with all the brains of a computer, without the screen*”, thus emphasising its educational and innovative intent to combine technology and learning in a playful and non-invasive format.

<sup>87</sup> Rapid7, R7-2015-27 and R7-2015-24: *Fisher-Price Smart Toy and HereO GPS Platform Vulnerabilities (FIXED)* (Rapid7 Blog, 2 February 2016), online at: <https://community.rapid7.com/community/infosec/blog/2016/02/02/security-vulnerabilitieswithin-fisher-price-smart-toy-hereo-gps-platform>).

<sup>88</sup> Shaped like a plush rocket, Grok contains an embedded “voice box” inside a zippered compartment and requires Wi-Fi connection via a companion app. To see the product: Curio Interactive Inc. 2024. Curio - AI Toys, <https://heycurio.com/>. accessed 05-07-2025.

<sup>89</sup> V. Pavliv, N. Akbari and I Wagner, ‘AI-powered smart toys: interactive friends or surveillance devices?’ in Proceedings of the 14th International Conference on the Internet of Things (IoT ‘24, ACM 2025) 172.

intentional commands but also background conversations, including external audio sources or nearby people. This raises privacy concerns, as sensitive information can be captured and transmitted without the user's knowledge. Furthermore, the toy's responses revealed vulnerabilities: although the experiment was not designed to elicit inappropriate content, some replies contained double meanings - for example, "*it's about spirit not size*". This suggests it may be possible to bypass or break out of the system prompt, allowing the toy to produce inappropriate or unsafe statements, representing a child safety risk and a potential avenue for manipulation.

Given the outlined and - not merely theoretical - cyber risks<sup>90</sup> the post-deployment phase must prioritize the implementation of robust cybersecurity safeguards<sup>91</sup>.

Article 15 of the AI Act mandates that high-risk systems - including those used in educational and play-based contexts<sup>92</sup> - be developed with a high degree of robustness and cybersecurity, aligned with the state of the art. This includes encryption, anomaly detection and protection against tampering. At a broader level, Article 5(1)(b) of the AI Act explicitly prohibits the use of AI systems that exploit vulnerabilities linked to age, thereby shielding children from manipulative or coercive behaviors.

Nevertheless, ensuring a secure post-deployment environment for children requires more than technical safeguards; it demands ongoing, structured monitoring and accountability throughout the system's lifecycle. As required by Article 71 of the AI

---

<sup>90</sup> See the BBC News article related to the Cayla doll case: <https://www.bbc.com/news/world-europe-39002142> (BBC, 2017), accessed 10 May 2025. Consider also that, where children's rights may be compromised, predefined sunsetting or withdrawal protocols should be established to ensure the safe decommissioning of harmful or outdated AI systems.

<sup>91</sup> In this context, it is important to consider that during the negotiations of the AI Act, numerous child rights organizations called for greater attention to the specific needs of children. In particular, they urged the inclusion of educational systems in the list of "*high-risk*" applications, the prohibition of AI practices that exploit vulnerabilities related to age and the development of clear guidelines to ensure transparency and comprehensibility of AI systems for children. While the final text of the AI Act has partially addressed these demands - by, for instance, including educational AI systems in Annex III and banning the use of AI that exploits age-related vulnerabilities - it has fallen short of explicitly recognizing children as a protected group in all provisions and it lacks specific instructions on how to communicate with child users. European Commission, "Commission Seeks Feedback on Guidelines on the Protection of Minors Online under the Digital Services Act" (11 March 2024).

<sup>92</sup> Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024, OJ L1689/1, Annex III.

Act, providers of high-risk AI must implement a post-market monitoring system to collect and assess performance data over time. Rather than a one-off evaluation, this should be seen as a living framework - one integrating technical vigilance with a sustained ethical responsibility to act in the best interests of the child.

Moreover, post-deployment oversight must be equipped to address adversarial threats, such as input manipulation or the covert reprogramming of educational agents for *non*-educational - or harmful - purposes<sup>93</sup>. To mitigate these risks, real-time monitoring systems must be capable of identifying not only technical malfunctions but also indicators of deliberate misuse, unauthorized alterations or manipulation, as these safeguards are essential to ensuring the long-term safety, reliability and trustworthiness of AI systems - provided they are effectively integrated within a continuous risk assessment framework<sup>94</sup>.

Central to this evaluation is the integration of the “Child Rights Impact Assessment” (hereinafter, CRIA): a methodology, applied from the design phase, that examines the potential impacts on children of laws, policies, programmes and services, and that can also be applied to assess both the potential and actual effects of AI systems on children’s rights<sup>95</sup>. The CRIA process begins with a screening stage to determine whether a policy, service or technology warrants a full assessment. Where significant impacts are identified, a full CRIA follows, starting with an analysis of the proposal’s scope and the relevant Articles of the UNCRC. This stage is backed by qualitative and quantitative evidence, including direct consultation feedback with children to ensure their views are considered and to identify recurring themes and priority concerns. The assessment then evaluates general and disproportionate impacts on specific groups of children and outlines corresponding mitigation strategies (*e.g.*: reduction in exposure to harmful content by X%). The process concludes with a set of findings, including

---

<sup>93</sup> For an in-depth investigation, see B. Guembe et al., ‘The Emerging Threat of AI-Driven Cyber Attacks: A Review’ (2022) 36(1) *Applied Artificial Intelligence* 2037254.

<sup>94</sup> NIST AI, Artificial Intelligence Risk Management Framework (*AI RMF 1.0*) (2023); URL: <https://nvlpubs.nist.gov/nistpubs/ai/nist.ai.100-1.pdf>.

<sup>95</sup> *Ex multis*, J. H. and M.A. Stephenson, ‘Human Rights Impact Assessment: Review and Practice Guidance for Future Assessments’ (2010) Scottish Human Rights Commission Report; L. Payne, ‘Child Rights Impact Assessment as a Policy Improvement Tool’ in K. Roberts Lyer (ed), *Human Rights Monitoring and Implementation* (Routledge 2020) 91.

recommendations and monitoring mechanisms. Publishing the CRIA enhances transparency and accountability, ensuring that AI systems are developed in a manner that upholds children's rights and delivers long-term, positive outcomes. Alongside this risk assessment approach, periodic impact reports should be mandated for high-risk AI systems, modeled after the "Data Protection Impact Assessments" (DPIAs), but tailored to specifically address child-specific risks, so that developers, providers, regulators and institutional users<sup>96</sup> must share clear, traceable responsibilities for the long-term impacts of AI on children's well-being.

Therefore, post-deployment accountability demands a collective responsibility from multiple stakeholders.<sup>97</sup> Indeed, regulators must define and enforce standards for an ongoing compliance, while civil society, academic and research institutions should serve as "watchdogs" and evaluators of AI's forthcoming impact and industry actors must commit to the long-term stewardship of their technologies. On this point, instruments such as the aforementioned AAR could play a role in ensuring that AI systems consistently meet children's rights and needs. It could serve as a tool for monitoring issues identified in earlier phases and facilitating the transfer of knowledge across different phases of the design and development. This ensures alignment among all stakeholders, enabling ongoing monitoring to maintain compliance throughout the product's lifecycle.

Ultimately, accountability must be understood not merely as a legal or procedural obligation, but as a moral and social responsibility. The best interests of the child, as enshrined in Article 3 UNCRC, can become an enforceable benchmark only if a "post-deployment conscience" is embraced - one that compels designers, developers and even decision-makers to measure AI's success, by its real-world impact on children's rights and well-being.

---

<sup>96</sup> Such as schools, public agencies and other stakeholders.

<sup>97</sup>T. Merlin, J. Boyd and C. Donovan, "The Role of Governments in Increasing Interconnected Post-Deployment Monitoring of AI" (2024) *arXiv preprint arXiv:2410.04931*.

## 5. Closing the lifecycle loop of child Rights-Based AI

And so, this story - one *about* and *for* children - almost comes to an end. It is a narrative where child agency, safety and protection form the hoped-for happy ending. Yet reality proves far more complex. Even when AI systems are designed, developed and deployed in line with children's rights standards, there is no guarantee of their continued compliance in real-world use. Here is where our story begins again, going back to the development phase or even to the design phase, in a never ending, possibly safe and child rights-based loop.

To be fully applicable, the lifecycle loop of child rights-based AI suggested in this work needs to address some limitations:

(i) *Existing frameworks* (e.g.: from UNICEF<sup>98</sup> and IEEE 2089-2021<sup>99</sup>) provide important guidelines to practitioners, but they often miss out on metrics and/or practical implementation tools. These gaps can pose limitations to their applicability, resulting in too high-level recommendations of difficult understanding and/or operationalization for practitioners. At the same time, few academic works, focusing on a specific case or system, rarely offer scalability solutions "*per se*". Consequently, core research priorities are: (i) identifying, evaluating and validating metrics and operational measures specifically for AI systems intended for children, and (ii) integrating these metrics and measures with knowledge from other fields (e.g.: development theories). At the same time, practitioners can in the meanwhile refer to valuable already existing materials. To guide the reflection, when creating and building a new service or product for children, practitioners can indeed refer to contributions

---

<sup>98</sup> UNICEF - V. Dignum, M. Penagos, K. Pigmans and S. Vosloo (November 2021).

<sup>99</sup> IEEE, Standard for an Age Appropriate Digital Services Framework Based on the 5Rights Principles for Children, (2021).

such as the ones highlighted above in this paper, or others like the 5Rights' "Playful by Design Toolkit"<sup>100</sup> or Save the Children's guide on "Child-Centered Design"<sup>101</sup>.

(ii) *Regulatory Sandboxes* are expected to be created in the EU by 2026<sup>102</sup>. Regulatory Sandboxes can be very effective tools to bridge the gap between technological innovation and slow regulatory adaptation. This gap is particularly evident in sectors such as fintech, AI, blockchain and biotech, where technology is advancing faster than regulators can regulate it. The sector concerning the protection of minors in the use of technology presents serious regulatory gaps, making it difficult to effectively safeguard the rights of young people in the digital environment. The Italian case is an emblematic example. Since the entry into force of the new European Electronic Communications Code<sup>103</sup> (December 2020), a derogation that allowed ICT companies to monitor and report child sexual abuse material online has lapsed. This regulatory gap has had direct and measurable consequences: reports to the competent authorities have decreased by 46% across Europe, negatively impacting prevention and enforcement efforts against child abuse. Furthermore, the "Caivano Decree" (September 2023)<sup>104</sup>, in an effort to strengthen child protection, delegated to AGCOM the task of defining technical tools for age verification and secure access to digital content. However, to date, no concrete implementing measures have been

---

<sup>100</sup> 5Rights Foundation, 'Playful by Design' (2021). <https://playfulbydesign.5rightsfoundation.com>. Accessed 11 September 2025.

<sup>101</sup> Save the Children Finland, 'Child-Centered Design' (2020). <https://resourcecentre.savethechildren.net/document/child-centered-design>. Accessed 11 September 2025.

<sup>102</sup> European Parliament and Council. Regulation (EU) 2024/1689 of the European parliament and of the council of 13 june 2024 laying down harmonised rules on artificial intelligence and amending regulations (ec) no 300/2008, (EU) no 167/2013, (EU) no 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (AI act) (text with eea relevance), 2024.

<sup>103</sup> Directive (EU) 2018/1972 establishing the European Electronic Communications Code [2018] OJ L321/36; transposed into Italian law by D. lgs., 8 november 2021, n. 207, GURI n.292, 9 December 2021.

<sup>104</sup> Decreto Legge 15 Settembre 2023, n°123 "Misure urgenti di contrasto al disagio giovanile, alla povertà educativa e alla criminalità minorile, nonché per la sicurezza dei minori in ambito digitale" <https://www.gazzettaufficiale.it/eli/id/2023/11/14/23A06292/sg> accessed 06 July 2025.

adopted: only guidelines are in force, which are not legally binding, and actual implementation by operators remains inconsistent. In this context, innovative tools such as AI regulatory sandboxes could represent a strategic opportunity to overcome the regulatory deadlock. Sandboxes offer a regulated yet flexible environment in which to test technologies and solutions (such as age verification systems, AI-based parental control, or the automated detection of illegal content) before their full legal application. The experience of the United Kingdom, for instance, shows how regulatory experimentation can contribute to the development of dedicated legislation. The UK Information Commissioner's Office (ICO) has used sandboxes to develop the principles of the "Children's Code", a legal framework that has since established new standards for the design of digital platforms with a focus on respecting children's rights.

However, so far, there are few examples of attempts to create such environments. A recent paper<sup>105</sup> proposes a regulatory framework for child-friendly AI sandboxes that integrates the EU AI Act with UNICEF guidelines and other international references (UN, OECD, UNESCO). This framework is structured around a multi-stakeholder, modular, and iterative process aimed at ensuring that the development and testing of AI systems respect the rights and well-being of children. Given the international relevance of the topic, interesting new contributions are expected in the near future;

(iii) *Zero risk doesn't exist*, cybersecurity threats may still emerge over time. Therefore, it is essential to move beyond voluntary guidelines and soft law (meaning, codes of conduct and non-binding recommendations). To ensure the long-term protection of children's rights in digital environments, companies must be encouraged - and, where necessary, compelled - to take shared responsibility through binding legal frameworks and effective enforcement mechanisms. In the post-deployment phase, proactive regulation is crucial to clearly define the duties and liabilities of AI producers, software developers and platform operators, with enforceable measures such as substantial fines for damages and explicit rights of claim for affected parties (*post-damage* protection). This ongoing accountability should be anchored in systematic monitoring, inspired by the CRIA or comparable methodologies, and guided by

---

<sup>105</sup>V. Charisi and V. Dignum, "Operationalizing AI Regulatory Sandboxes for Children's Rights and Well-Being" in Human-Centered AI (Chapman and Hall/CRC 2024) 231.

robust indicators. Relevant measures may include: (i) tracking the number and severity of cyber-incidents involving children, (ii) assessing the speed and effectiveness of responses to identified risks, (iii) evaluating the participation of children in post-deployment reviews, (iv) analysing the distribution of impacts across different groups of children in order to detect disproportionate effects, and (v) collecting data on children's own perceptions of safety and well-being when engaging with digital systems. Embedding such evidence-based indicators within regulatory frameworks ensures that accountability extends beyond the design stage, turning compliance into a continuous, transparent and participatory process that protects children's rights throughout the entire life cycle of AI systems.

Also, future efforts should aim to overcome these limitations by developing more effective strategies for engaging children directly - such as through interviews, surveys and focus groups - and by fostering a collaborative approach that integrates diverse professional and academic expertise. This strategy will better position the final AI system to meet security standards and ensure compliance with children's rights and related obligations.



## LA TUTELA DEL MINORE NELL'ERA DELL'INTELLIGENZA ARTIFICIALE: QUESTIONI APERTE SUL METODO DI GESTIONE DEL RISCHIO

Matilde Ratti\*

### Abstract

La diffusione di sistemi di intelligenza artificiale evidenzia la crescente esigenza di individuare soluzioni di protezione per il minore e i suoi diritti. Sul punto, le diverse normative volte alla tutela dei minori *online*, sia nell'uso di strumenti di intelligenza artificiale sia nella fruizione dei *social network* o nel trattamento dei dati personali, presentano approcci eterogenei riconducibili a differenti metodologie regolatorie. Sono numerosi i punti di contatto tra le criticità affrontate dai provvedimenti sull'impiego di strumenti dotati di intelligenza artificiale, di protezione dei dati personali e di uso dei *social network*. Anche a livello normativo, dal modello statunitense, alla legislazione australiana alla recente normativa italiana, le principali questioni attengono al grado di effettività delle misure individuate nella gestione del rischio per i minori nell'ambiente digitale.

*The wide application of artificial intelligence systems highlights the growing need to identify solutions to protect minors and their rights. In this regard, the various regulatory initiatives aiming to protect minors in the digital environment, including both those related to the use of artificial intelligence tools, and the use of social networks, and the processing of personal data, highlight heterogeneous approaches answering to different regulatory methodologies. There are indeed several points of contact between the critical issues addressed by the provisions on the use of artificial intelligence tools, personal data protection, and the use of social networks. Even at the regulatory level, from the US model to Australian framework, and the recent Italian legislation, the main issues concern the degree of effectiveness of the measures identified in managing risks for minors in the digital environment.*

---

\* Professoressa Associata di diritto privato, Università di Bologna, [matilde.ratti@unibo.it](mailto:matilde.ratti@unibo.it)

Il presente contributo è stato sottoposto a referaggio a doppio cieco ed è finanziato su progetto *Children as Vulnerable Users of IoT and AI-based Technologies: A Multi-level Interdisciplinary Assessment* – CURA, PRIN 2022–2022KAEWYF, – Next Generation EU; CUP: J53D23005540006.

## Indice Contributo

LA TUTELA DEL MINORE NELL'ERA DELL'INTELLIGENZA ARTIFICIALE: QUESTIONI APERTE SUL METODO DI GESTIONE DEL RISCHIO .....	266
Abstract.....	266
Keywords.....	267
1. Il minore e l'accesso agli strumenti dotati di intelligenza artificiale.....	267
2. La protezione dei dati personali volta alla tutela del minore che interagisca con strumenti di IA.....	269
3. La protezione dei dati e la tutela del minore nell'accesso ai <i>social network</i> : profili di analogia.....	271
4. Le regole in materia <i>age verification</i> quali strumenti trasversali di tutela.....	275
5. La recente legge italiana sull'impiego degli strumenti di IA .....	281
6. Considerazioni conclusive: verso un approccio trasversale alla tutela del minore <i>online</i> ? .....	284

## Keywords

Minore – Intelligenza Artificiale – Protezione dei Dati Personalii – Piattaforme Digitali – Age Verification

### 1. Il minore e l'accesso agli strumenti dotati di intelligenza artificiale

La crescente consapevolezza circa gli effetti dell'uso dei dispositivi che consentano l'accesso ad Internet, ai *social media* e ai sistemi dotati di intelligenza artificiale sta

plasmando lo scenario politico-legale sul tema del minore che agisce *online*<sup>1</sup>. Alcune tematiche suscitano un particolare interesse poiché presentano evidenti rischi per il minore in quanto tale e, tra queste, vi è certamente quella connessa alla possibilità di avere rapido accesso agli strumenti dotati di intelligenza artificiale. Sul piano internazionale, il Comitato sui diritti dell'infanzia delle Nazioni Unite è intervenuto con il Commento Generale n. 25 esplicitamente estendendo l'ambito di applicazione dei diritti del fanciullo ad Internet (e alle nuove tecnologie) e ribadendo la doverosa attenzione da prestare alla fragilità ontologicamente connessa alla natura del minore<sup>2</sup>. Sebbene tale approccio sia penetrato in certa misura negli atti normativi dell'Unione Europea<sup>3</sup>, confermando la rilevanza del tema nell'attuale cultura legislativa, non vi è ad oggi una disciplina europea specificamente rivolta alla protezione del minore che

---

<sup>1</sup> Tra le più recenti opere che affrontano in modo specifico il tema, cfr. D. Amram, *Non ho l'età ma... Costruire competenze abilitanti per una società dell'informazione a prova di (in)capacità del minore di età* (1° ed., Lefebvre Giuffré 2025); C. Camardi, 'Relazione di filiazione e *privacy*. Brevi note sull'autodeterminazione del minore' (2018) 5 Jus Civ 831ss.; R. Senigaglia, 'L'identità personale del minore di età nel cyberspazio tra autodeterminazione e *parental control system*' (2023) 6 NLCC, 1568ss.; G. Carapezza Figlia, 'Sharing: nuovi conflitti familiari e rimedi civili' (2023) 5 NGCC 1104ss.; A. La Spina, 'L'identità del minore nella realtà on-life tra protezione e autodeterminazione' (2024) 10 Famiglia e Diritto, 920ss.; I. Garaci, 'Il «superiore interesse del minore» nel quadro di uno sviluppo sostenibile dell'ambiente digitale' (2021) 4 NLCC, 800ss.; M. Giandoriggio, 'I minori d'età e i social network: l'insostenibile leggerezza del post' (2024) 3 Danno e resp. 296ss.; I. Garaci, 'La *privacy* del minore d'età nell'ambito familiare' (2023) 1 EJPLT 84ss.; L. Lenti, 'L'identità del minorenne' (2006) 1 NGCC 68ss.; E. Moscati, 'Il minore nel diritto privato, da soggetto da proteggere a persona da valorizzare (contributo allo studio “interesse del minore”)' (2014) 10 Dir. fam. pers. 1141ss.

<sup>2</sup> Comitato sui diritti dell'infanzia, *Commento generale n. 25: Sui diritti dei minorenni in relazione all'ambiente digitale*, 2022 <[I diritti dei minorenni in relazione all'ambiente digitale | UNICEF Italia](https://www.unicef.it/it/minorenni/ambiente-digitale)> ultimo accesso 1 settembre 2025.

<sup>3</sup> Alcune delle enunciazioni contenute in tale Commento sono state recepite anche nei considerando del Digital Services Act (DSA). In particolare, il considerando 71 sottolinea che la protezione dei minori costituisce un obiettivo politico prioritario dell'Unione europea e definisce le condizioni in cui una piattaforma *online* può considerarsi accessibile ai minorenni, richiedendo ai prestatori l'adozione di misure appropriate e proporzionate, anche attraverso interfacce progettate secondo logiche di *privacy* e sicurezza "by design" e "by default". In stretta connessione, il considerando 81 stabilisce che le piattaforme e i motori di ricerca di dimensioni molto grandi sono tenuti a considerare, nell'analisi dei rischi sistematici, l'impatto delle proprie interfacce e dei propri servizi sui diritti del minore, con particolare attenzione ai possibili effetti pregiudizievoli sullo sviluppo fisico, mentale e morale, nonché ai meccanismi che possono sfruttare l'inesperienza o la vulnerabilità dei minorenni. Infine, il considerando 89 riafferma la necessità di modellare il *design* dei servizi digitali nel rispetto del superiore interesse del fanciullo e prevede che i meccanismi di tutela e di ricorso offerti dal regolamento siano resi effettivamente accessibili anche ai soggetti minorenni. Tali previsioni riprendono e traducono in chiave normativa europea alcune delle linee direttive poste dal Commento Generale n. 25, che insiste sulla necessità di una protezione specifica dei minori nell'ambiente digitale, nonché sul riconoscimento del loro diritto a strumenti adeguati, trasparenti e accessibili di partecipazione e tutela.

utilizzi sistemi di intelligenza artificiale. Infatti, sebbene il Regolamento europeo 2024/1689 (l'*AI Act*) vietи l'impiego di sistemi che sfruttino le vulnerabilità (anche quando siano connesse all'età)<sup>4</sup> e preveda obblighi di valutazione del rischio che tengano conto la natura dell'utilizzatore<sup>5</sup>, il tema del minore non è trattato in modo specifico né è oggetto di una disciplina dedicata. Ci si propone, dunque, di valutare l'opportunità di un approccio organico alla tutela dei diritti del minore partendo da un'analisi delle più rilevanti decisioni in materia e indagando, in seguito, le potenzialità e le criticità delle primissime soluzioni giuridiche adottate nell'ordinamento italiano e in altri Stati che, in modo più o meno diretto, si sono interessati al tema<sup>6</sup>.

## **2. La protezione dei dati personali volta alla tutela del minore che interagisca con strumenti di IA**

Nello scenario italiano, i primi provvedimenti ad interessarsi della tutela del minore che adoperi strumenti dotati di intelligenza artificiale sono proprio quelli del Garante per la protezione dei dati personali, che ha indagato l'opportunità di implementare sistemi di verifica dell'età (o *age verification*) per l'accesso a servizi *online* allo scopo di limitare la potenziale violazione dei diritti del minore. Ci si riferisce in primo luogo al noto provvedimento del 2 febbraio 2023<sup>7</sup>, avente ad oggetto il sistema *Replika*, una *chatbot* intelligente che genera un “amico virtuale” a supporto del benessere emotivo dell'utente, a più riprese oggetto dell'attenzione del Garante. Nel caso in commento,

---

<sup>4</sup> Cfr. AI Act, art. 5, par. 1, lett. b), Peraltro, l'art. 7 dell'*AI Act* attribuisce alla Commissione il potere di adottare atti delegati per modificare i casi d'uso dei sistemi di IA ad alto rischio se questi presentano « un rischio di danno per la salute e la sicurezza, o di impatto negativo sui diritti fondamentali» (cfr. lett. b) del par. 1) anche tenendo conto del criterio secondo il quale «esiste uno squilibrio di potere o le persone che potrebbero subire il danno o l'impatto negativo si trovano in una posizione vulnerabile rispetto al *deployer* di un sistema di IA, in particolare a causa della condizione, dell'autorità, della conoscenza, della situazione economica o sociale o dell'età» (par. 2, lett. h).

<sup>5</sup> Cfr. AI Act, art. 9, par. 9.

<sup>6</sup> EDPB, *Linee guida 8/2020 sul targeting degli utenti di social media* (2021). In dottrina, ampiamente in G. Finocchiaro, *Intelligenza Artificiale. Quali regole?*, (1<sup>a</sup> ed., Il Mulino 2024); G. Finocchiaro, ‘La proposta di Regolamento sull'Intelligenza Artificiale: il modello Europeo basato sulla gestione del rischio’ (2022) 2 Dir. inform. Inf. 303ss.; G. Finocchiaro, ‘Il perfezionamento del contratto on line: opportunità e criticità’ (2018) 1-2 Dir. com. scambi internaz., 187ss.; G. Finocchiaro, *La protezione dei dati personali in Italia – Regolamento UE n. 2016/679 e d.lgs. 10 agosto 2018, n. 101* (1<sup>a</sup> ed., Zanichelli Editore 2019).

<sup>7</sup> Prov. del 2 febbraio 2023 [2023] GPDP 9852214, Registro dei provvedimenti n. 39 del 2 febbraio 2023.

l'Autorità aveva evidenziato la necessità che il *provider* adottasse dei meccanismi di verifica dell'età per consentire l'utilizzo della *chatbot*<sup>8</sup>. La società implementava dunque un meccanismo di *age gate* in tutte le pagine di registrazione, prevedeva un periodo di raffreddamento (*cooling-off period*) e predisponiva strumenti per consentire agli interessati l'esercizio effettivo dei propri diritti<sup>9</sup>. Due anni dopo, tali misure erano giudicate insufficienti con il provvedimento del 10 aprile 2025<sup>10</sup>, che chiariva la prospettiva giuridica adottata dall'Autorità. Considerato che proprio secondo le ricostruzioni della Società il servizio sarebbe stato destinato a soli maggiorenni, il trattamento dei dati del minore avrebbe violato il generalissimo principio di minimizzazione previsto dal Regolamento 2016/679 (in seguito semplicemente "GDPR"). Il trattamento avrebbe inoltre violato gli obblighi di *accountability* incombenti sul *provider* (art. 24 del GDPR) e avrebbe comportato l'ingiusta esposizione del minore ad un servizio inadeguato alla sua età<sup>11</sup>.

Un'analogia posizione era emersa anche nel 2024 in riferimento ad un altro provvedimento storico della medesima Autorità, quello avente ad oggetto il servizio di ChatGPT<sup>12</sup>. In questo caso, il Garante rilevava la mancanza di un sistema per

---

<sup>8</sup> La registrazione, infatti, richiedeva unicamente l'inserimento di nome, indirizzo *e-mail* e genere, senza alcuna procedura di *age verification*. Il Garante aveva inoltre rilevato la mancanza di un sistema di moderazione dei contenuti calibrato in base all'età dell'utente, con la conseguenza che i minorenni risultavano esposti a materiali non adeguati al loro grado di sviluppo. Per completezza, si segnala altresì che in mancanza di informativa sul trattamento dei dati personali l'Autorità ha segnalato l'impossibilità di comprendere le modalità del trattamento e la base giuridica dello stesso. Sul punto, il Garante ha escluso che, per i minori, la base giuridica potesse rinvenirsi nell'accettazione delle condizioni di utilizzo, stante l'incapacità legale a contrarre per la fruizione del servizio.

<sup>9</sup> La misura della limitazione del trattamento ordinata dall'Autorità era in seguito sospesa dal medesimo Garante. *Provvedimento del 22 giugno 2023* [2023] GPDP 10013893, Registro dei provvedimenti n. 280 del 22 giugno 2023.

<sup>10</sup> Cfr. *Provvedimento del 10 aprile 2025* [2025] GPDP 10130115, Registro dei provvedimenti n. 232 del 10 aprile.

<sup>11</sup> Cfr. *irid*: «Nello specifico, la mancata adozione da parte della Società di misure idonee a salvaguardare l'accesso e l'utilizzo del servizio Replika aveva comportato non solo che Luka trattasse, sistematicamente, dati personali ulteriori rispetto a quelli realmente necessari per conseguire la finalità del trattamento (vale a dire offrire il servizio ad utenti maggiorenni), ma anche che tale trattamento riguardasse dati relativi a soggetti vulnerabili (minorenni, potenzialmente di età anche inferiore ai 13 anni) che, a causa di tale carenza ed attesa la tecnologia innovativa sottesa al servizio e la natura altamente sensibile delle conversazioni fornite dal chatbot, sono stati esposti ad un rischio particolarmente elevato».

<sup>12</sup> *Provvedimento del 2 novembre 2024* [2024] GPDP 10085455, Registro dei provvedimenti n. 659 del 2 novembre 2024. La decisione si inserisce a chiusura della vicenda che aveva coinvolto la Società OpenAI in relazione ai trattamenti di dati personali condotti tramite la sua IA *ChatGPT*. Con primo provvedimento del 30 marzo 2023, doc. web n. 9870832, il Garante aveva cominato la sanzione di limitazione del trattamento dei dati personali degli interessati stabiliti in Italia sulla base di una serie di violazioni intercorse. Spiccavano, in particolare, un *data breach* avvenuto nel marzo 2023, consistente nella visualizzazione da parte degli utenti del servizio di dati personali appartenenti ad altri utilizzatori; l'assenza di informativa adeguata sul sito *web* e la mancanza di meccanismi per garantire i diritti di opposizione e cancellazione degli interessati; l'assenza di base giuridica del trattamento per l'addestramento degli algoritmi sottesi al funzionamento della piattaforma. La sanzione

verificare la provenienza del consenso dall'esercente la responsabilità genitoriale<sup>13</sup>, consenso richiesto dal *provider* proprio per utilizzare il servizio<sup>14</sup>. Da un lato, l'obbligo di verifica dell'età era posto in capo al titolare del trattamento, ovverosia il *provider*: questi avrebbe dovuto verificare l'età dell'utente con la necessaria diligenza. Dall'altro, l'Autorità ammetteva che il contratto stipulato tra l'infraquattordicenne (con il permesso del genitore) e il *provider* per l'uso del servizio *ChatGPT* potesse costituire un'idonea base giuridica per trattare i dati personali del minore ai sensi del GDPR. Inoltre, pur considerando le diverse caratteristiche del servizio rispetto a quello esaminato nel provvedimento in precedenza richiamato, il Garante anche in questo caso evidenziava il rischio di esposizione del minore a contenuti inappropriati<sup>15</sup> ed individuava quale soluzione sostanziale l'imposizione di un vincolo di accesso a ChatGPT tramite la precostituzione di un idoneo meccanismo di *age verification*.

### **3. La protezione dei dati e la tutela del minore nell'accesso ai *social network*: profili di analogia**

Nel medesimo periodo in cui il Garante italiano affrontava le questioni sul minore che acceda a strumenti dotati di intelligenza artificiale, negli Stati Uniti d'America era

---

communata era stata poi sospesa con *Provvedimento dell'11 aprile 2023*, 874702, a seguito dell'adozione di misure organizzative e tecniche da parte della società volte ad adeguare il trattamento dei dati personali alle previsioni normative.

<sup>13</sup> Ancora a titolo di completezza, interessante la replica della Società, avallata dal Garante, che, con riferimento alla mancata adozione di misure idonee per verificare il consenso prestato dai minori, nega l'applicazione dell'art. 8 GDPR in quanto la base giuridica del trattamento non sarebbe rinvenibile tanto nel consenso degli interessati, quanto nell'esecuzione di un contratto ai sensi dell'art. 6 lett. b) GDPR.

<sup>14</sup> La decisione, a ben vedere, si pone in contraria direzione rispetto a quanto l'Autorità stessa aveva in precedenza stabilito nel citato Provvedimento del 2 febbraio 2023 in relazione al servizio Replika. In quell'occasione, il Garante aveva escluso *a priori* che la base giuridica potesse rinvenirsi nell'esecuzione di adempimenti nell'ambito di un contratto concluso con l'utente, stante l'incapacità del minore a contrarre nell'ordinamento.

<sup>15</sup> Con riguardo alle modalità di verifica dell'età, la società aveva vagliato alcune misure correttive, quali l'inserimento dei dati di una carta di credito, l'introduzione di appositi meccanismi di IA in grado di misurare l'età, la scansione della carta di identità prima dell'accesso al servizio. OpenAI aveva infine deciso di affidare l'attività ad una società esterna (Yoti), la quale avrebbe restituito ad OpenAI solo l'esito positivo o negativo della verifica previo autoscatto dell'utente e scansione di un documento di identità. Tale sistema è stato tuttavia giudicato insufficiente dall'Autorità. In aggiunta, per ciò che qui interessa ai fini della delineazione di un sistema di responsabilità in merito all'accesso al servizio da parte di minore, si evidenzia che la sanzione è stata comminata al titolare per aver mantenuto esposti i minori al rischio di contenuti inappropriati per un determinato periodo di tempo. Non è peraltro accolta la posizione di OpenAI che imputa alla mancanza di standard uniformi sulle misure più idonee per la tutela dei minori, ritenendo il Garante che la responsabilità di individuare le soluzioni idonee alla tutela del minore caso per caso ricada sul titolare del trattamento.

adottato il Provvedimento della *Federal Trade Commission* del 2 agosto 2024<sup>16</sup> sull'adeguatezza del trattamento di dati personali di minori svolto dalla Bytedance, proprietaria di TikTok, alle disposizioni del *Children's Online Privacy Protection Act* (COPPA, 15 U.S.C. 6501) e del *Children's Online Privacy Protection Rules* (16 C.F.R. Part 312). Seppur adottato nei confronti di un *social network*, il provvedimento appare incentrato su un tema assai vicino a quello in esame, avendo ad oggetto il trattamento automatizzato dei dati personali degli utenti minorenni (anche con finalità di *marketing*). Nel *social* era consentito che minori di 13 anni creassero *account* personali. In particolare, al momento dell'apertura del profilo erano raccolti nomi, indirizzi *e-mail*, numeri di telefono e immagini, dati successivamente ritenuti eccedenti rispetto a quanto consentito dalla normativa applicabile. Secondo quanto evidenziato dalla *Federal Trade Commission*, infatti, la Sezione 312.4(c) delle COPPA Rules prevedeva che il *provider* potesse raccogliere solo alcuni dati del minore prima di ottenere il consenso da parte dell'esercente la responsabilità genitoriale e, comunque, solo al fine di consentire il funzionamento del servizio. Inoltre, come nei casi oltreoceano, era rilevato che il sistema di verifica dell'età dell'utente fosse facilmente aggirabile tramite, ad esempio, una falsa dichiarazione di età o accedendo al *social* attraverso piattaforme terze (come Google o Instagram) che non prevedevano, a loro volta, rigidi sistemi di verifica dell'età<sup>17</sup>. Il procedimento, ancora pendente presso la *Federal Trade Commission* e dall'esito è incerto, pone il problema – se non ancora dal punto di vista legislativo, quantomeno in via di valutazione di opportunità sociale – della possibilità per il minore di agire liberamente in rete sui *social network* e lascia emergere la stretta connessione esistente tra le preoccupazioni avanzate dall'Autorità per la protezione dei dati personali italiana nei confronti dei prestatori di sistemi di IA e la *Federal Trade Commission* in relazione ai prestatori di *social network*. Il fulcro di entrambe le questioni sta proprio nell'applicazione del principio di minimizzazione del trattamento dei dati e nell'appropriatezza degli strumenti normativi e tecnici previsti nell'ipotesi in cui il minore possa accedere ad ambienti virtuali ove, a seconda del caso specifico, potrebbero anche essere utilizzati sistemi di intelligenza artificiale.

---

<sup>16</sup> Federal Trade Commission, *Provvedimento Bytedance Ltd, Us v.* (2024), <<https://www.ftc.gov/legal-library/browse/cases-proceedings/bytedance-ltd-us-v>> ultimo accesso 17 settembre 2025

<sup>17</sup> È stata inoltre rilevata la mancanza di un'informativa adeguata che spiegasse quali dati personali dei minori trattasse e per quale finalità, violando le Sezioni 312.3(a) e 312.4(d) delle COPPA Rules e non è stato richiesto il consenso da parte dei genitori, violando così le Sezioni 312.3(b) e 312.5(a)(1) COPPA Rules

Dell'assenza di misure per la tutela dei minori nei *social network* si sono interessati anche altre autorità per la protezione dei dati personali. In particolare, nell'agosto 2022, l'Autorità irlandese aveva adottato un progetto preliminare di decisione<sup>18</sup> nei confronti di TikTok Technology Limited riguardante l'assenza di strumenti in grado di proteggere il minore sulla piattaforma. Il progetto di decisione si concentrava sulla possibile violazione di alcune delle norme in materia di protezione dei dati personali previste dal GDPR<sup>19</sup>. In particolare, l'Autorità irlandese rilevava la mancanza di un sistema di *parental control*, l'assenza di informazioni circa la diffusione dei contenuti pubblicati dai minori e la carenza di protezione dei profili da questi creati, impostati di *default* come *account* "pubblici" e tramite un sistema di verifica dell'età consistente nella semplice dichiarazione espressa dall'utente al momento dell'iscrizione. A seguito delle osservazioni poste da TikTok sul progetto di provvedimento, l'Autorità irlandese condivideva il progetto anche con l'Autorità tedesca e con quella italiana, le quali presentavano alcune obiezioni<sup>20</sup>. L'Autorità irlandese deferiva dunque la controversia all'EDPB, che interveniva con decisione vincolante<sup>21</sup>. Era così stabilito che la società avesse violato alcune delle norme del GDPR richiamate, ma non l'art. 25 del GDPR in materia di *privacy by design* e *by default*, disposizione solitamente invocata in funzione dell'accertamento di un trattamento di dati eccessivo. Cionondimeno, era osservato il mancato rispetto del principio di correttezza nell'omettere di comunicare al minore le potenzialità di diffusione dei dati personali che questi avrebbe caricato sulla piattaforma<sup>22</sup>. Il Garante irlandese escludeva, a cascata, la violazione dell'art. 25 GDPR, ma ordinava a TikTok di provvedere all'inserimento di una notifica a comparsa durante la registrazione e la pubblicazione di video, riconoscendo il rischio

---

<sup>18</sup> Data Protection Commission, *In the matter of TikTok Technology Limited: Decision of the Data Protection Commission made pursuant to Section 111 of the Data Protection Act 2018 and Articles 60 and 65 of the General Data Protection Regulation*, (IN-21-9-1 2023) <[final decision tiktok in-21-9-1 - redacted 8 september 2023.pdf](https://www.dataprotection.ie/documents/2023/09/21/21-9-1-final-decision-tiktok-in-21-9-1-redacted-8-september-2023.pdf)> ultimo accesso 18 settembre 2025.

<sup>19</sup> In particolare, si trattava degli artt. 5, 12, 13, 24, 25 GDPR.

<sup>20</sup> Anche queste avevano infatti segnalato la violazione delle stesse norme del GDPR da parte di TikTok.

<sup>21</sup> EDPB, *Decisione vincolante 2/2023 relativa alla controversia presentata dall'autorità di controllo irlandese riguardante TikTok Technology Limited (articolo 65 del RGPD)* (2023) <[edpb bindingdecision 202302 ie sa ttl children it 0.pdf](https://edpb.europa.eu/documents/2023/02/23/2302-0-edpb-bindingdecision-202302-0-children-it-0.pdf)> ultimo accesso 17 febbraio 2025.

<sup>22</sup> Preme osservare che l'EDPB nega la violazione dell'art. 25 non in punto di diritto, ma in quanto ritiene che le informazioni presentate dall'Autorità irlandese circa l'assenza di ulteriori misure adottate dal prestatore per la verifica dell'età sono insufficienti a stabilire se le soluzioni adottate da TikTok siano inadatte a tutelare i minori. Cfr. EDPB, *Decisione vincolante 2/2023*, (n 21) 58.

per il minore che utilizzasse la piattaforma<sup>23</sup>. La misura di tutela prescelta era dunque volta alla maggiore sensibilizzazione del minorenne e del genitore nei confronti dei potenziali rischi di utilizzo del *social network*, pur non risultando violato il principio di *privacy by design* e *by default*<sup>24</sup>.

A ben vedere una simile posizione, di delicato equilibrio, è emersa proprio nel provvedimento ChatGPT sopra richiamato, nel quale l'Autorità italiana, pur ordinando la predisposizione di misure tecniche per la tutela del minore, aveva negato l'applicabilità dell'art. 8 GDPR, sostenendo che il consenso a cui tale norma si riferisce non costituisse la legittima base giuridica per il trattamento dei dati personali svolto, con la conseguenza che la sua ipotetica violazione sarebbe risultata in concreto irrilevante.

L'esame dei provvedimenti pone in primo luogo in luce le evidenti incertezze connesse ad un processo, attualmente in atto, di definizione del quadro normativo applicabile. Tutti i provvedimenti citati riconoscono il rischio di ingiusta esposizione del minore e la necessità di adottare idonee misure tecnologiche, di processo o di trasparenza, atte a limitare tale rischio. Nello scenario europeo, non è tuttavia chiarita la norma o il principio di diritto violato. In effetti, il riferimento all'art. 8 GDPR in materia di consenso prestato dall'esercente la responsabilità genitoriale in caso di minore che utilizzi servizi *online* presenta il limite dell'applicabilità materiale della previsione, letteralmente confinata ai casi nei quali la base giuridica da porre a fondamento del trattamento sia proprio il consenso. Tale norma non sarebbe dunque applicabile qualora la base del trattamento dei dati (come precisato dal Garante nel caso ChatGPT) fosse da individuarsi nella conclusione di un contratto tra l'utente del servizio (ancorché tramite il consenso espresso dai soggetti esercenti la responsabilità genitoriale) ed il prestatore titolare del trattamento. Evidenziare un trattamento che non rispetti il *principio di privacy by design* o *privacy by default* (con conseguente violazione dell'art. 25 GDPR) potrebbe costituire una soluzione giuridicamente più appropriata in astratto, considerata la natura ontologicamente elastica dei principi di diritto citati, ma l'EDPB non pare ad oggi confermare la soluzione prospettata dal Garante irlandese. Ciò nondimeno, in tutti i provvedimenti richiamati, è evidente il ricorso alle

---

<sup>23</sup> Il Garante irlandese, con provvedimento 1° settembre 2023, irroga quindi la sanzione di euro 345 milioni ritenendo violati gli artt. 5, 12, 13 e 24 GDPR. Cfr. Data Protection Commission, *In the matter of TikTok Technology Limited* (n 18).

<sup>24</sup> Cfr. EDPB, *Decisione vincolante 2/2023* (n 21) 67.

previsioni in materia di protezione dei dati personali allo scopo di affrontare il tema della tutela del minore. Si osserva, inoltre, che tale tendenza è trasversale ai casi di impiego dei sistemi intelligenti e dei *social media*.

La seconda osservazione che si può svolgere discende proprio da quest'ultima circostanza, nel senso che l'illecito trattamento dei dati, le modalità di accesso al servizio e i derivanti rischi di utilizzo per il minore appaiono intersecare scenari e strumenti assai differenziati. In altre parole, non si tratta solo di impiego di strumenti intelligenti, né unicamente di illecito trattamento dei dati personali o di improprio utilizzo dei *social network*. Spesso, le problematiche in ordine alla tutela del soggetto altamente vulnerabile possono sussistere a prescindere dalla tipologia di servizio prestato e riguardano le modalità di trattamento dei dati personali degli utenti, così come il rischio di esporli a contenuti o servizi inadeguati alla loro età<sup>25</sup>. Analogamente, e in modo logicamente conseguente, la misura alla quale più sovente i Garanti volgono la loro attenzione pare quella connessa alla limitazione di accesso alla rete, alla piattaforma, al *social network* o allo strumento di IA.

#### **4. Le regole in materia *age verification* quali strumenti trasversali di tutela**

Le norme in materia di limitazione dell'accesso in ragione dell'età appaiono dunque uno strumento trasversale nell'intento di garantire tutela al minore. Il punto di contatto evidenziato spinge a valutare positivamente l'opportunità di estendere il presente ambito di indagine. Ciò pare utile per più ragioni. In primo luogo, le norme sui *social network* e minori sono state adottate in un'epoca precedente (seppur non distante) a quella attuale, nella quale ci si interroga anche sul più recente tema dell'intelligenza artificiale. L'antecedenza storica, seppur minima, è certamente di interesse poiché consente di esaminare le tendenze legislative e gli orientamenti decisionali che si sono formati in relazione ai *social network*, sì da verificarne l'utilità e l'efficacia rispetto all'eventuale normazione in materia di intelligenza artificiale. In secondo luogo, l'estensione dell'ambito di indagine pare utile in ragione di alcune osservazioni di carattere operativo, in quanto da un lato i *provider* potrebbero trovarsi ad impiegare strumenti dotati di intelligenza artificiale proprio nella fornitura dei loro servizi. Dall'altro, la stretta connessione tra le tematiche è altresì data dalla circostanza

---

<sup>25</sup> Ibid.

che tali strumenti potrebbero comunque essere resi disponibili tramite l'identificazione svolta proprio dai *social network*.

Con riferimento a tali fornitori, nello scenario europeo è utile richiamare il *Digital Services Act*<sup>26</sup> e, in particolare, l'art. 28<sup>27</sup>. La norma stabilisce l'obbligo in capo ai fornitori di piattaforme *online* di adottare misure adeguate e proporzionate a garantire un elevato livello di tutela dei minori<sup>28</sup>. Tra i progetti avviati dalla Commissione europea volti all'attuazione di questa previsione<sup>29</sup> rientra il recente *Statement 1/2025* dell'EDPB a tutela dei minori nell'ambiente digitale, che pure caldeggi l'adozione di sistemi di *age assurance* allo scopo di realizzare un bilanciamento tra gli obblighi derivanti dal diritto dell'Unione europea e il rispetto del GDPR<sup>30</sup>. In particolare, l'atto è indirizzato ai fornitori di servizi *online* (piattaforme, siti, applicazioni, operatori

---

<sup>26</sup> Regolamento (UE) 2022/2065 del Parlamento Europeo e del Consiglio del 19 ottobre 2022 relativo a un mercato unico dei servizi digitali e che modifica la direttiva 2000/31/CE (regolamento sui servizi digitali) [2022] OJ L277/1.

<sup>27</sup> Sul punto, la Commissione Europea ha reso disponibile un modello tecnico di verifica dell'età volto a proteggere i minori *online*. Si veda <[Commission releases enhanced second version of the age-verification blueprint | Shaping Europe's digital future](#)> ultimo accesso 18 settembre 2025.

<sup>28</sup> La norma dà inoltre la possibilità alla Commissione di adottare orientamenti in merito. Reg. (UE) 2022/2065, art. 28, par. 1 e 4: «I fornitori di piattaforme *online* accessibili ai minori adottano misure adeguate e proporzionate per garantire un elevato livello di tutela della vita privata, di sicurezza e di protezione dei minori sul loro servizio. [...] La Commissione, previa consultazione del comitato, può emanare orientamenti per assistere i fornitori di piattaforme *online* nell'applicazione del paragrafo 1».

<sup>29</sup> Giova inoltre evidenziare che i progetti avviati dalla Commissione inerenti all'individuazione di meccanismi di verifica dell'età ai sensi dell'art. 28 DSA si intrecciano anche con l'esigenza dell'Unione di sviluppare soluzioni di Portafoglio europeo di Identità Digitale (PEID). La Commissione, infatti, intende vagliare la possibilità che un domani gli attributi relativi “all'età anagrafica” possano essere condivisi dall'utente europeo anche tramite il PEID, nel caso in cui i prestatori di servizi siano tenuti a verificare l'età. Da <[Commission releases enhanced second version of the age-verification blueprint | Shaping Europe's digital future](#)>: «The age verification blueprint lays the groundwork for broader deployment of age-appropriate services in the future. It is also referred to as the ‘mini-wallet’, as it is built on the same technical specifications as the forthcoming European Digital Identity Wallets, ensuring long-term compatibility and providing a stepping stone toward the rollout of the European Digital Identity Wallets before the end of 2026».

<sup>30</sup> EDPB, *Dichiarazione 1/2025 sulla garanzia dell'età* (2025) <[edpb statement 20250211ageassurance\\_it.pdf](#)>. Il Garante europeo ha stabilito che i sistemi di *age assurance* debbano essere conformi ai principi sanciti dal GDPR, in particolare necessità, proporzionalità, minimizzazione dei dati, correttezza e trasparenza. L'implementazione deve fondarsi su un'idonea base giuridica di cui all'articolo 6 GDPR (ed eventualmente, ove rilevante, su una delle eccezioni di cui all'articolo 9, paragrafo 2), ed essere preceduta, nei casi di trattamenti ad alto rischio, dalla redazione di una valutazione d'impatto *ex articulo 35* GDPR. È fatto divieto che l'*age assurance* si traduca in attività ulteriori rispetto alla finalità propria di verifica dell'età, quali identificazione, localizzazione o profilazione degli utenti, in violazione dei principi di limitazione della finalità e di minimizzazione del trattamento. I dati trattati devono essere limitati agli attributi strettamente necessari a dimostrare il superamento o meno di una determinata soglia anagrafica, anche attraverso soluzioni di tokenizzazione o tecniche crittografiche. Infine, i titolari e i responsabili del trattamento sono tenuti ad adottare un quadro di *governance* che assicuri la piena *accountability* ai sensi dell'articolo 5, paragrafo 2, GDPR, garantendo tracciabilità delle decisioni, la possibilità di svolgere *audit* dei processi e la possibilità di controllo da parte delle autorità competenti.

digitali) che devono limitare l'accesso dei minori o offrire contenuti e servizi adeguati alla loro età. Questi, unitamente ai fornitori dei servizi di verifica dell'età (*Identity Provider*) dovrebbero limitare l'accesso a contenuti vietati o non appropriati, adottare misure specifiche contro le differenti casistiche di rischio (a titolo esemplificativo abusi, *grooming*, violenza, pornografia, etc.) e attivare sistemi di *parental control* e segnalazione.

A livello internazionale, la maggior parte delle regolamentazioni a tutela dei minori *online* suddividendo la responsabilità e l'onere della tutela del minore tra l'apparato latamente statuale, le famiglie (sovente tramite meccanismi di richiesta del consenso al genitore) e le imprese (tramite meccanismi di autoregolamentazione e previsione di obblighi di diversa natura)<sup>31</sup>. Nella gran parte degli scenari, il minore può, tramite meccanismi più o meno stringenti, navigare *online*, ma la sua capacità naturale o giuridica è limitata da meccanismi di acquisizione del consenso dell'esercente la responsabilità genitoriale.

In Inghilterra, è stato adottato l'*Online Safety Act* nel 2023<sup>32</sup>, il quale prevede una serie di adempimenti precauzionali in capo ai fornitori dei servizi *online* per la valutazione dei rischi sulla base di una logica progressiva decrescente, secondo la quale più intense misure sono necessarie al diminuire dell'età del minore. I servizi interessati sono quelli che pongono in contatto gli utenti tra loro (i cd. *user-to-user services*) e i servizi di ricerca (i cd. *Search services*). Entrambi devono adottare misure proporzionate per mitigare i rischi per i bambini e proteggere le diverse fasce d'età da contenuti dannosi<sup>33</sup>. Sul punto, le modalità di attuazione di tali *duty of care* sono esplicitate nel Children's Code

---

<sup>31</sup> Anche la Legge sulla Protezione dei Minori della Repubblica Popolare Cinese (中华人民共和国未成年人保护法) del 17 ottobre 2020 demanda ai genitori la regolamentazione dell'utilizzo della rete e l'accesso dei minori a Internet, attribuendo tuttavia un rilevante ruolo nella formazione dei minori anche allo Stato e alle scuole. La normativa, in vigore dal 1° giugno 2021, sottolinea fortemente il ruolo dell'alfabetizzazione digitale dei minori e impone in capo allo Stato e alle famiglie il compito di prevenire il fenomeno di indipendenza da Internet. Una disciplina specifica è inoltre prevista per i fornitori di servizi *online* di gioco, i quali sono tenuti ad adottare misure per limitare l'accesso dei minori. A titolo esemplificativo, la legge prevede l'istituzione di un sistema di autenticazione elettronica dell'identità e la classificazione dei giochi offerti sulla base degli standard nazionali. I fornitori sono inoltre tenuti a fornire suggerimenti adatti all'età dell'utente e ad adottare misure tecniche per non consentire ai minori di accedere a giochi o funzioni di gioco inappropriate. Ulteriore misura prevista consiste nel vietare la fornitura ai minori di giochi *online* in capo ai fornitori dalle 22:00 alle 8:00 del giorno successivo.

<sup>32</sup> *Online Safety Act* 2023 del 26 ottobre 2023.

<sup>33</sup> Rileva in particolare il *Chapter 2* «Providers of user-to-user services: duties of care», la cui *Section 12* dispone verso i fornitori l'obbligo di implementare politiche chiare nei termini di servizio per garantire la sicurezza dei bambini.

ad opera dell'Autorità garante inglese (*Information Commissioner's Office* – più brevemente “ICO”)<sup>34</sup>. Per limitare l'accesso ai contenuti vietati, gli operatori possono avvalersi di specifici meccanismi di verifica dell'età previsti dall'Autorità, che vanno dall'autodichiarazione all'impiego di documenti di identificazione<sup>35</sup>. Il *Children's Code* distingue poi cinque fasi di sviluppo (ad es. fase di pre-alfabetizzazione, adolescenziale etc.) in relazione ai quali gli operatori sono tenuti ad adottare diversi approcci precauzionali<sup>36</sup>. Sono previste regole sulla trasparenza e di limitazione delle tecniche manipolatorie. In particolare, vengono posti limiti al cosiddetto *nudge*, l'uso di tecniche per guidare o incoraggiare bambini a fornire dati personali non strettamente necessari come, ad esempio l'impiego di colori specifici per favorire associazioni mentali. È necessario adottare misure che rendano evidenti eventuali operazioni di raccolta o registrazione dei dati personali, tramite luci o segnali visivi<sup>37</sup>.

Anche negli Stati Uniti sono previste numerose indicazioni in merito alla trasparenza. L'impianto normativo in materia si compone di due diversi atti, il *Children's Online Privacy Protection Act* del 1998, 15 U.S.C. 6501–6505 (in seguito semplicemente “COPPA Act”) e il part 312—*Children's Online Privacy Protection Rule* (in seguito solo “COPPA Rule”). La normativa COPPA prevede una serie di obblighi per prestatori di servizi *online*, che possono essere distinti in obblighi di trasparenza e di diligenza. Ad esempio, quanto alla trasparenza, i *provider* sono tenuti a fornire un avviso riguardo alle informazioni raccolte sul minore, alle modalità con cui si domanda al genitore il

---

<sup>34</sup> Information commissioner's officer, *Children's code* (2020) <[Age appropriate design: a code of practice for online services | ICO](https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/age-appropriate-design-a-code-of-practice-for-online-services/)> consultato il 17 settembre 2025.

<sup>35</sup> Il *Children's code*, Section 3, fa riferimento a diversi metodi di verifica dell'età. Sono annoverati: l'autodichiarazione, sulla base della quale gli utenti dichiarano autonomamente la loro età senza fornire alcuna prova ulteriore; l'uso di sistemi di IA, che in base all'analisi delle interazioni dell'utente è in grado di stimare l'età; il ricorso a servizi di verifica di terze parti, le quali si impegnano a non raccogliere dati sensibili; la conferma da parte del titolare adulto avente un *account* presso lo stesso servizio; l'uso di misure tecniche che scoraggino dichiarazioni false, come il blocco automatico di *account* ripetutamente non confermati; l'uso di documenti di identificazione, che consentano di confermare l'età. L'ICO ha cura, tuttavia, di precisare che tale ultimo metodo appare sproporzionato rispetto all'esigenza di tutelare i minori, in quanto produrrebbero impatti eccessivi sulla *privacy* dell'utente.

<sup>36</sup> Le differenti fasce si suddividono in: 0 – 5 anni, periodo della pre-alfabetizzazione e sviluppo iniziale; 6 – 9 anni, periodo dell'apprendimento scolastico di base; 10 – 12 anni, anni di transizione; 13 – 15 anni, adolescenza iniziale; infine, 16 - 17 anni, periodo dell'avvicinamento all'età adulta. La tabella che consente di individuare le capacità cognitive dei minori per ogni fascia d'età è disponibile *online*: <<https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/age-appropriate-design-a-code-of-practice-for-online-services/annex-b-age-and-developmental-stages/>>

<sup>37</sup> Ad esempio, una luce che si accende quando il dispositivo sta registrando.

consenso al loro impiego, il loro utilizzo e le pratiche di divulgazione<sup>38</sup>. I genitori devono avere la possibilità di accedere ai dati raccolti sui figli<sup>39</sup>. Ancora, è fatto divieto di condizionare la partecipazione a giochi o attività alla fornitura di informazioni personali non necessarie<sup>40</sup>. Il COPPA prevede poi la possibilità di aderire a programmi *Safe Harbour* disciplinati dal § 312.11, uno strumento di autoregolamentazione volontaria per i *provider*, proposti da gruppi industriali o soggetti privati e approvati dalla *Federal Trade Commission* (FTC) qualora garantiscano protezioni equivalenti o superiori a quelle stabilite dalla normativa<sup>41</sup>. Nello scenario statunitense, si precisa, il divieto di accedere<sup>42</sup> ai siti internet per i minori di 13 anni è strutturato come una mera possibilità per il *provider*.

Nell'opposta direzione si muove invece l'*Online Safety Act* australiano del 2021<sup>43</sup> che, alla Sezione 63 D, definisce come *age restricted social media platform*, ossia come

---

<sup>38</sup> Children's Online Privacy Protection Rule 16 CFR Part 312 §312.4(b): «*Direct notice to the parent*. An operator must make reasonable efforts, taking into account available technology, to ensure that a parent of a child receives direct notice of the operator's practices with regard to the collection, use, or disclosure of personal information from children, including notice of any material change in the collection, use, or disclosure practices to which the parent has previously consented».

<sup>39</sup> Children's Online Privacy Protection Rule 16 CFR Part 312, § 312.6(a)(1)): «Upon request of a parent whose child has provided personal information to a website or online service, the operator of that website or online service is required to provide to that parent the following: A description of the specific types or categories of personal information collected from children by the operator, such as name, address, telephone number, email address, hobbies, and extracurricular activities».

<sup>40</sup> Children's Online Privacy Protection Rule 16 CFR Part 312, §312.7: «An operator is prohibited from conditioning a child's participation in a game, the offering of a prize, or another activity on the child's disclosing more personal information than is reasonably necessary to participate in such activity».

<sup>41</sup> Alcuni dei progetti attualmente in corso sono reperibili al seguente link <<https://www.ftc.gov/enforcement/coppa-safe-harbor-program>> ultimo accesso: 14 marzo 2025.

<sup>42</sup> L'indicazione è reperibile tra le FAQ del COPPA: «Can I block children under 13 from my general audience website or online service? Yes. COPPA does not *require* you to permit children under age 13 to participate in your general audience website or online service, and you may block children from participating if you so choose. By contrast, you may not block children from participating in a website or online service that is directed to children as defined by the Rule, even if the website or online service is also directed to users age 13 or older».

<sup>43</sup> Online Safety Act 2021, come modificato da Act No. 127, 2024. L'Online Safety Act 2021 (OSA) intende assicurare che Internet rimanga uno spazio sicuro intervenendo secondo due linee di azione: la prima consiste nell'attribuire ampi poteri di controllo all'Autorità garante australiana (*eSafety Commissioner*), la quale assume un ruolo attivo nei rapporti tra i prestatori di servizi *online* e gli utenti; la seconda consiste nell'individuare le cd. «Expectations» nei confronti dei prestatori di servizi per garantire un ambiente digitale sicuro (*Part 4 – Basic online safety expectations*), senza tuttavia entrare nello specifico delle modalità con le quali tali «Expectations» possono essere raggiunte. Con riferimento alla prima linea di azione, ai sensi del *Part 3 – Complaints, objections and investigations, Division 1- Introduction, No. 29 ss.*, i minori possono rivolgersi direttamente al *Commissioner* lamentando episodi di cyberbullismo o segnalando contenuti a loro vietati. Il *Commissioner* può, a sua volta, ai sensi del *Part 5, No 65 e No. 109*, emettere un avviso di rimozione al fornitore di *social media* qualora l'oggetto dei contenuti sia stato accertato essere in violazione dell'OSA; inoltre, ai sensi del *No. 49 e No. 56*, può richiedere ai prestatori un «*periodic reporting notice*» sullo stato di conformità alle cd. «Expectations». Sono infine previsti

piattaforme *online* vietate ai minori di 16 anni<sup>44</sup>, quei servizi elettronici<sup>45</sup> che consentono l'interazione tra due o più utenti o che consentono di caricare materiali *online*<sup>46</sup>. Il divieto in esame è di natura sostanziale. In altre parole, a differenza di

---

ulteriori poteri per il controllo della compliance e monitoraggio (*Part 10 -Enforcement*). Con riferimento alla seconda linea d'azione, il legislatore australiano prevede gli obiettivi che i prestatori devono raggiungere per garantire un ambiente digitale sicuro (*Part 4, Division 2 – Basic online safety expectations, No. 46 Core Expectations*), delegando ai codici di condotta la definizione delle modalità tecniche ed organizzative per raggiungerli. La *Part 9 – Online content scheme* definisce comunque uno schema minimo che tali codici di condotta devono seguire, specificando i contenuti vietati ai minori di diciotto anni (*No. 106 – 107*) e fornendo esempi di “argomenti” da disciplinare nei codici. A titolo esemplificativo, la *Subdivision B—General principles relating to industry codes and industry standards, No. 138 “Examples of matters that may be dealt with by industry codes and industry standards”* prevede che i codici di condotta debbano individuare le procedure atte sia ad assicurare che gli account *online* non possano essere creati dai minori senza il consenso dei genitori sia a fornire ai genitori informazioni circa i modi e gli strumenti con cui possono monitorare o controllare l'attività dei propri figli sui loro servizi. Anche nella redazione di tali codici di condotta si prevede un diretto coinvolgimento del *Commissioner*, che può aggiornare gli indirizzi degli standard tecnici ed organizzativi da adottare, gli ambiti nei quali i codici devono intervenire, ed organizzare delle consultazioni pubbliche al fine di agevolare la stesura dei codici di condotta (*Part 9, Division 7, Subdivision C – E*). L'approccio che traspare è di mantenere la sfera d'azione pubblica separata dalla sfera d'azione privata. In altre parole, il legislatore australiano dell'OSA 2021 non intende obbligare in concreto il prestatore a determinati “comportamenti” nella prestazione del suo servizio, limitandosi piuttosto a fissare i risultati che i prestatori di servizi devono raggiungere attraverso proprie scelte d'azione.

<sup>44</sup> Giova precisare che la *Part 4A - Social media minimum age*, adottata il 2 dicembre 2024 con l'*Act No. 127, 2024* e in vigore a partire dal 10 dicembre 2025, è l'unica parte del testo normativo australiano che impone direttamente l'obbligo a determinati prestatori di vietare l'accesso ai loro servizi ai minori di 16 anni. In tale contesto normativo si inseriscono inoltre le eSafety Commissioner, *Basic Online Safety Expectations* (2024) in <[Federal Register of Legislation - Online Safety \(Basic Online Safety Expectations\) Determination 2022](#)> ultimo accesso 14 febbraio 2025. “*The Expectations*” integrano l'OSA attraverso l'individuazione più specifica di misure standard minime che i fornitori di servizi devono assicurare per il raggiungimento dei risultati previsti dalla *Part 4 OSA*.

<sup>45</sup> La normativa si concentra sui *social network*, ma al contempo prevede norme specifiche qualora siano impiegati sistemi di IA. Nella *Division 2 – Basic Online safety expectations, Section 8A “Additional expectations—provider will take reasonable steps regarding generative artificial intelligence capabilities* vi è espresso rimando all'adozione di misure in grado di consentire solo un utilizzo sicuro di IA generativa per tutti. Tuttavia, mentre a Settembre 2024, il *Commissioner* australiano ha formalmente richiesto a YouTube, Facebook, Instagram, TikTok, Snap, Reddit, Discord e Twitch di indicare quali meccanismi di *age assurance* avessero adottato, nessuna richiesta in tal senso è stata avanzata nei confronti di fornitori di sistemi di IA. In eSafetyCommissioner, *eSafety calls on social media giants to reveal just how many Aussie kids are signing up* (2024) <[eSafety calls on social media giants to reveal just how many Aussie kids are signing up | eSafety Commissioner](#)> consultato il 14 febbraio 2025.

<sup>46</sup> Specificamente, le piattaforme che vi rientrano sono: «(a) an electronic service that satisfies the following conditions: (i) the sole purpose, or a significant purpose, of the service is to enable online social interaction between 2 or more end users; (ii) the service allows end users to link to, or interact with, some or all of the other end users; (iii) the service allows end users to post material on the service; (iv) such other conditions (if any) as are set out in the legislative rules; OR (b) an electronic service specified in the legislative rules but does not include a service mentioned in subsection. For the purposes of subparagraph (1)(a)(i), online social interaction includes online interaction that enables end-users to share material for social purposes». È inoltre previsto che il *provider* di tali piattaforme non possa raccogliere strumenti identificativi emessi dallo Stato australiano né utilizzare servizi di accreditamento previsti dal Digital IA Act del 2024. Cfr. OSA, s(63DB): «A provider of an age restricted social media platform must not: (a) collect government issued identification material; or (b) use an accredited service (within the meaning of the Digital ID Act 2024); for the purpose of complying with section 63D, or for purposes that include the purpose of complying with section 63D». In altre parole, la piattaforma non può avvalersi né delle carte di identità rilasciate nell'ambito del Commonwealth, né

quanto prevede l'art. 8 del GDPR o, seppur in maniera graduata, la normativa britannica, il legislatore australiano non si limita ad imporre il rispetto di regole in materia di accesso, capacità giuridica o moderazione dei contenuti, bensì vieta in modo radicale l'impiego di tali piattaforme ai minori di 16 anni. La responsabilità non è in questo caso allocata in capo al genitore, ma vi è una chiara scelta di politica legislativa che riconosce a priori la rischiosità dell'impiego dei *social media*.

## 5. La recente legge italiana sull'impiego degli strumenti di IA

Nello scenario italiano, il tema della tutela del minore è stato recentemente oggetto di specifica normazione. A differenza di quanto è avvenuto in Australia con riferimento alla limitazione dell'uso dei *social network*, ove il legislatore ha scelto di imporre un limite di natura sostanziale con riferimento allo specifico servizio, la legge del 23 settembre 2025, n. 132 (Legge sull'IA) ha adottato un approccio più mediato, che appare ispirato dall'art. 8 del GDPR. L'art. 4 della Legge sull'IA, astenendosi da valutazioni circa la rischiosità del mezzo, prevede infatti che «l'accesso alle tecnologie di intelligenza artificiale dei minori di anni quattordici richied[a] il consenso di chi esercita la responsabilità genitoriale»<sup>47</sup>. Tale formulazione sembra poter includere l'accesso ai sistemi di IA tramite ogni tipo di piattaforma o fornitore, privilegiando la

---

utilizzare servizi di identità digitale. La Sezione 63DB, *Use of certain identification material and services*, prevede infatti che per «government issued identification material» sia da intendersi «identification documents issued by the Commonwealth, a State or a Territory, or by an authority or agency of the Commonwealth, a State or a Territory (including copies of such documents); and (b) a digital ID (within the meaning of the Digital ID Act 2024) issued by the Commonwealth, a State or a Territory, or by an authority or agency of the Commonwealth, a State or a Territory». È inoltre previsto dalla *Section 63DA* che il Ministero per le Comunicazioni possa individuare con propri provvedimenti quali informazioni le *social media platform* non devono raccogliere per assolvere all'obbligo.

<sup>47</sup> Cfr. L. 132/2025, art. 4 c. 4: «L'accesso alle tecnologie di intelligenza artificiale da parte dei minori di anni quattordici nonché il conseguente trattamento dei dati personali richiedono il consenso di chi esercita la responsabilità genitoriale, nel rispetto di quanto previsto dal regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, e dal codice in materia di protezione dei dati personali, di cui al decreto legislativo 30 giugno 2003, n. 196. Il minore di anni diciotto, che abbia compiuto quattordici anni, può esprimere il proprio consenso per il trattamento dei dati personali connessi all'utilizzo di sistemi di intelligenza artificiale, purché le informazioni e le comunicazioni di cui al comma 3 siano facilmente accessibili e comprensibili». Sempre nello scenario europeo, lo Stato del Vaticano ha adottato con Decreto n. DCCII le *Linee guida in materia di intelligenza artificiale* (2024) <[Linee guida in materia di intelligenza artificiale del Governatorato dello Stato della Città del Vaticano](#)> ultimo accesso: 17 settembre 2025. Pur non entrando nell'ambito della tutela dei minori, le linee guida intendono promuovere uno sviluppo ed uno utilizzo di sistemi di IA in ottica antropocentrica, con ciò adeguandosi alla direzione intrapresa dal legislatore europeo. Sebbene con formulazione differente, sono infatti presenti sia gli stessi divieti disposti dall'art. 5 AI Act sia l'obbligo di rispettare i principi di trattamento dei dati personali nell'ambito dello sviluppo ed utilizzo del sistema di IA.

natura particolare del minore e la sua fragilità. La scelta circa l'idoneità del servizio o del prodotto dotato di IA è dunque rimessa in primo luogo al *provider* che lo renda disponibile sul mercato. Qualora il servizio non fosse dichiaratamente ritenuto adeguato al minore infraquattordicenne, sarebbe poi il genitore o l'esercente la responsabilità a poter rendere il consenso al suo utilizzo. Da ultimo si osserva che, come è avvenuto per l'art. 8 GDPR nei provvedimenti sopra richiamati, l'onere di consentire l'applicazione in concreto della disposizione ricadrà (in una misura che occorrerà determinare) sul *provider* che (in modo autonomo o tramite un *Identity Provider*) predisporrà il sistema di riconoscimento del genitore o, in ottica di minimizzazione, di *age verification* del minore, prima, e dell'esercente la responsabilità genitoriale poi.

Quanto all'effettività della previsione, il ruolo degli *Identity Provider* è evidentemente cruciale e, nello scenario italiano, è già stato declinato con riferimento ad uno specifico settore nella delibera dell'AGCOM 96/25/CONS<sup>48</sup> di attuazione dell'art. 13-*bis* del Decreto Caivano<sup>49</sup>. Si tratta della norma che impone ai fornitori di piattaforme che diffondono in Italia «immagini e video a carattere pornografico» di verificare la maggiore età degli utenti, allo scopo di «evitare l'accesso a contenuti pornografici da parte di minori degli anni diciotto». La delibera dell'AGCOM ha un contenuto del tutto specifico e settorialmente indirizzato, in quanto contiene obblighi diretti ai soggetti che diffondono in Italia contenuti pornografici. Tuttavia, in relazione alla corrente analisi, pare utile evidenziare le osservazioni formulate dall'Autorità in merito alle soluzioni tecniche per la limitazione dell'accesso ai servizi citati, in quanto appaiono potenzialmente rilevanti ognqualvolta ci si accinga ad imporre un sistema di *age limitation* in relazione ad un servizio, sia questo quello del *social network* o quello

<sup>48</sup> AGCOM, *Delibera 96/25/CONS: adozione delle modalità tecniche e di processo per l'accertamento della maggiore età degli utenti in attuazione della legge del 13 novembre 2023, n. 159* (2025) <[delibera 96-25-CONS.pdf](https://www.agcom.it/contenuti/legge-13-novembre-2023-delibera-96-25-cons.pdf)> ultimo accesso 17 settembre 2025: «In via di premessa, è importante sottolineare che la Commissione ha condiviso l'obiettivo perseguito da Agcom attraverso il progetto notificato inteso a proteggere i minori *online*, in particolare dai contenuti a carattere pornografico, che possono nuocere alla loro salute e al loro sviluppo fisico, mentale e morale. Si tratta, infatti, di obiettivi allineati a quelli del quadro giuridico europeo per i servizi online, in particolare il regolamento (UE) 2022/2065 (di seguito il «regolamento sui servizi digitali o DSA») e la direttiva 2000/31/CE (direttiva sul commercio elettronico)».

<sup>49</sup> D.l. 15 settembre 2023, n. 123, art. 13-*bis*: «I gestori di siti web e i fornitori delle piattaforme di condivisione video, che diffondono in Italia immagini e video a carattere pornografico, sono tenuti a verificare la maggiore età degli utenti, al fine di evitare l'accesso a contenuti pornografici da parte di minori degli anni diciotto. [...] L'Autorità per le garanzie nelle comunicazioni stabilisce, [...] con proprio provvedimento, sentito il Garante per la protezione dei dati personali, le modalità tecniche e di processo che i soggetti di cui al comma 2 sono tenuti ad adottare per l'accertamento della maggiore età degli utenti».

connesso all’impiego di un sistema dotato di intelligenza artificiale. Pur non imponendo univoche soluzioni tecnologiche, l’AGCOM ha rilevato rischi trasversali connessi alla previsione di *age gate*, raccomandando che a procedere alla verifica dell’età siano soggetti terzi rispetto al gestore del servizio e scoraggiando i prestatori dall’avvalersi di meccanismi interni per la verifica dell’età<sup>50</sup>. Si tratta del sistema del “doppio anonimato”, secondo il quale da un lato i dati personali dell’utente devono essere tutelati nei confronti della piattaforma che offre il servizio e, dall’altro, i siti visitati non possono essere conosciuti dall’*Identity Provider*. Da ultimo, non può non evidenziarsi come nella delibera emerga altresì la valutazione dell’Autorità sull’efficacia della soluzione tecnica proposta: nessuno dei sistemi di *age verification* è considerato completamente sicuro rispetto a meccanismi elusivi da parte degli utenti<sup>51</sup>.

---

<sup>50</sup> L’Autorità non esclude, poi, che tale verifica potrà essere soddisfatta, a partire dal 2026, anche con il PEID. Infatti, i nuovi *digital wallet* potranno essere in grado di condividere anche solo l’attributo dell’età anagrafica con i prestatori di servizi, senza per ciò stesso rivelare l’identità dell’utente. Cfr. Allegato B) alla delibera n. 96/25/CONS cit., 14: «Nella maggior parte dei casi, i cittadini non possono scambiare digitalmente a livello transfrontaliero, in modo sicuro e con un livello elevato di protezione dei dati, informazioni relative alla loro identità quali indirizzi, età e qualifiche professionali, patenti di guida e altri permessi e dati di pagamento. Pertanto, l’EUDI *wallet* consentirebbe di superare tali limiti offrendo la possibilità di scambiare attributi minimi dell’identità necessari ad accedere determinati servizi online per cui è richiesta l’autenticazione, come ad esempio la prova dell’età. Inoltre, il nuovo Regolamento eIDAS prevede che, qualora le piattaforme online di dimensioni molto grandi, come definite dal DSA, impongano agli utenti di autenticarsi per accedere ai servizi online, queste dovranno accettare anche l’uso dei portafogli europei di identità digitale, rigorosamente su richiesta volontaria dell’utente, anche per quanto riguarda gli attributi minimi necessari per lo specifico servizio online per il quale è richiesta l’autenticazione, come la prova dell’età». L’allegato riporta anche il rapporto del regolatore inglese OFCOM, che si è espresso in relazione all’*Online Safety Act*. L’autorità inglese ha ritenuto che la verifica dell’età tramite PEID sia altamente efficace. L’AGCOM non ritiene, invece, che lo SPID possa considerarsi una soluzione ottimale, almeno fino a quando i relativi prestatori avranno accesso alle informazioni circa i siti visitati dagli utenti che richiedono l’identificazione. Cfr. Allegato A), Delibera 96/25/CONS, cit., 4-5: «[...] tale sistema di autenticazione SPID consente all’*Identity Provider* di conoscere il particolare sito/piattaforma visitato dall’utente e non è da escludere che tale informazione venga memorizzata all’interno dei sistemi dell’*Identity Provider*. [...] Si evidenzia, pertanto, la possibilità, con un sistema pubblico, di poter disporre in breve tempo di un insieme di *Identity Provider* certificati e di una rete di connessioni e accordi (basati su obblighi normativi esistenti), in grado di fornire, all’utente e per il tramite di questo alla piattaforma, la cosiddetta prova dell’età. Quanto detto vale sia per la modalità di verifica dell’età collegate a sistemi di verifica dell’età non basati su applicativi installati nel terminale utente sia per quelli basati su applicativi installati nel terminale utente (cosiddetti *digital wallet*), fermo restando la necessità di preservare la libertà di scelta dell’utente in merito all’utilizzo di uno o dell’altro sistema, anche considerando la potenziale invasività dell’installazione di determinate app sul proprio dispositivo personale. L’Autorità, pertanto, solo laddove soddisfatti i requisiti di cui alla sezione seguente sul doppio anonimato (protezione dei dati personali nei confronti del sito/piattaforma e non conoscenza del sito visitato/piattaforma da parte dell’*Identity Provider*), ritiene che sistemi pubblici siano utilizzabili».

<sup>51</sup> Allegato A), Delibera 96/25/CONS, cit., 10: «Per quanto riguarda i dispositivi attualmente offerti sul mercato, diversi regolatori evidenziano che attualmente tutte le soluzioni proposte possono essere in qualche modo aggirate. Ad esempio, l’utilizzo di una VPN, che nasce per garantire sicurezza nell’utilizzo di Internet agli utenti,

## 6. Considerazioni conclusive: verso un approccio trasversale alla tutela del minore *online*?

Le soluzioni normative esaminate in materia di tutela del minore *online*, sia che questo utilizzi sistemi di intelligenza artificiale, *social network* o che semplicemente coincida con il soggetto interessato del trattamento dei dati personali, possono essere raggruppate per metodologie. Mentre Stati Uniti e Regno Unito hanno adottato approcci basati rispettivamente sulla co-regolamentazione e sulla valutazione del rischio, senza prevedere specifici divieti, l’Australia ha introdotto un divieto sostanziale in merito all’uso dei *social network* ai minori di sedici anni. L’Italia e l’Europa sembrano aver adottato una posizione intermedia. L’art. 28 del DSA impone un obbligo sui prestatori di servizi *online* di garantire «un elevato livello di tutela» per il minore. Con riferimento all’accesso agli strumenti dotati di intelligenza artificiale, nel solo scenario italiano, è da ultimo stato attribuito al soggetto esercente la responsabilità genitoriale il compito di acconsentire a che il minore vi sia esposto, mentre è allocata sul *provider* la responsabilità di implementare un sistema di verifica<sup>52</sup> della provenienza del consenso dal soggetto legittimato ad esprimere o di verifica dell’età del minore *tout court*. Appare corretto l’approccio del legislatore europeo (e italiano) nell’astenersi dall’individuare un metodo specifico per lo svolgimento dell’*age verification*, dimostrando di intendere che di una rincorsa tra metodi di verifica e sviluppo tecnologico potrebbe trattarsi in concreto.

In ognuno dei casi qui richiamati, però, l’efficacia in concreto delle norme che si pongono l’obiettivo di limitare l’accesso agli strumenti dotati di intelligenza artificiale, ai *social network* o al trattamento dei dati personali *online*, è subordinata alla possibilità tecnica di aggirare il divieto. Come anticipato, l’AGCOM conferma che tutte le soluzioni tecniche per garantire la sicurezza dei processi di *age verification* esaminate nella Delibera 26/95/CONS. si prestano, ad oggi, a meccanismi elusivi mediante l’uso di VPN da parte degli utenti. A ben vedere, la medesima conseguenza è trasversale a

---

può allo stesso tempo consentire a un minore di eludere un sistema di verifica dell’età. Il soggetto tenuto, ai sensi della legge, a realizzare il sistema di controllo dell’età per l’accesso ai contenuti, non deve promuovere o fare comunque riferimento a qualsiasi meccanismo di elusione dei sistemi di *age assurance*.

<sup>52</sup> Già oggi obbligatoriamente basato sul sistema del doppio anonimato per quanto concerne il ristretto ambito di applicazione della Delibera 96/25/CONS.

tutti i sistemi normativi esaminati, sia nel caso in cui non sia previsto alcun limite di utilizzo per i minori (quando questo venga ad esempio imposto dal *provider*), sia nel caso in cui vi sia l'imposizione di un divieto assoluto di utilizzo (come nel caso australiano), sia nel caso in cui la scelta circa la possibilità di accedere al servizio venga affidata al consenso del genitore (come prevedono la legge italiana ed il GDPR). In ognuna delle situazioni richiamate, il minore che voglia aggirare il divieto si scontrerà con le misure di sicurezza adottate dal fornitore del servizio e, a seconda dell'ordinamento, dall'*Identity Provider*.

Ne consegue la necessità di approcciare la questione della tutela del minore non solo dal punto di vista legislativo e prescrittivo, ma anche a livello culturale, includendo nel dialogo non solo i legislatori ma gli stessi *provider*. Ad accrescere il livello generale di consapevolezza dei consociati circa i rischi connesso all'utilizzo dell'IA *online*, accentuati dall'intrinseca fragilità del minore, possono contribuire alcuni strumenti, già evidenziati nei provvedimenti esaminati, quali le tecniche anti *nudge*, i processi di co-regolamentazione con gli stessi fornitori e, pur con i limiti già emersi negli studi in materia di protezione dei dati personali, i sistemi di notifica informativa (si pensi al provvedimento Tik Tok). Tuttavia, una riflessione di carattere culturale sui rischi per i minori che utilizzino strumenti di IA, non può prescindere dal considerare, al contempo, i rischi impliciti e connessi all'accesso e all'impiego di questi strumenti *online*. Dati i numerosi livelli di sovrapposizione che possono esistere tra le attività svolte dai minori sui *social media*, quando accedono a strumenti dotati di intelligenza artificiale e quando divengono interessati del trattamento dei dati personali, oltre a regole puntuali nei differenti settori di interesse sembra utile prendere in considerazione una visione più ampia, quella del minore, soggetto vulnerabile, che agisce *online*. L'esame dei rimedi emersi nei differenti ordinamenti sia a livello normativo (emergono gradualmente limiti di età e divieti d'accesso) sia provvidenziale (i rischi rilevati nell'esame di casistiche apparentemente dissimili appaiono i medesimi) ha infatti posto in luce come, in tutti gli scenari esaminati, il rischio evidenziato e la relativa misura correttiva siano direttamente collegati al momento in cui il minore accede al servizio che, in molti casi, coincide con la possibilità per questi di accedere *online*. A prescindere dal settore, deve dunque emergere la consapevolezza che la vulnerabilità del minore è descritta in relazione a rischi condivisi (in modo più o meno acuto a seconda della specifica tipologia dello

strumento o dei servizi utilizzati) quando questi accede alla rete, luogo di amplificazione dei diritti, ma anche delle vulnerabilità.